LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

ETÄHALLINTA 3G-REITITTIMELLÄ

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2011
Sakari Nikander

Lahden ammattikorkeakoulu
Tietotekniikka

NIKANDER, SAKARI: Etähallinta 3G-reitittimellä

Tietoliikennetekniikan opinnäytetyö, 46 sivua, 15 liitesivua

Syksy 2011

TIIVISTELMÄ

Tämä opinnäytetyö tehdään Kouvolassa toimivalle DD-Control-yritykselle, joka tarjoaa langattomasti etähallittavia automaatioratkaisuja ohjelmoitavilla logiikoilla. Opinnäytetyössä käsitellään langattoman etähallinnan mahdollistamista ja optimointia 3G-reitittimellä (Third Generation). Opinnäytetyössä tutkitaan ja vertaillaan kahta 3G-reititintä ja niiden soveltuvuutta etähallintaan. Tavoitteena on myös tutkia lisäantennien vaikutusta muodostettavaan 3G-yhteyteen.

3G-tekniikalla tarkoitetaan kolmannen sukupolven matkapuhelintekniikoita, joista Euroopassa yleisimmin käytetty tekniikka on UMTS (Universal Mobile Telecommunications System). UMTS käyttää laajakaistaista koodijakotekniikkaa, joka mahdollistaa teoreettisen 2 Mbit/s maksimisiirtonopeuden. UMTS-verkko koostuu runkoverkosta, radioliityntäverkosta ja päätelaitteista. Suomen UMTS-verkot käyttävät 900- ja 2100-taajuuskaistoja. Alkuperäistä release 99:n version UMTS-verkkoa on kehitetty entistä tehokkaammaksi käyttämällä HSPA-tekniikkaa (High Speed Packet Access), jonka uusimmat versiot mahdollistavat jopa teoreettisen 42 Mbit/s maksiminopeuden. UMTS-verkon päätelaitteet käyttävät erilaisia antennityyppejä, joita ovat esimerkiksi suunta-antennit ja ympärisäteilevät antennit. Yleisimmät 3G-reitittimien tietoturvaominaisuudet ovat pakettisuodatus ja VPN-tuki (Virtual Private Network).

3G-reitittimien ominaisuuksia vertaamalla huomataan selvä ero suunnitelluilla käyttötarkoituksilla. Laitteissa käytettävä 3G-tekniikka eroaa huomattavasti, mikä vaikuttaa jonkin verran laitteiden käyttöönottoon. Antennimittauksista voidaan todeta, että suunta-antenni ei ole yleisesti tarpeellinen kaupunkiseudulla. 3G-reitittimien tietoturvaominaisuudet eroavat VPN-tuella. Muodostetaan eri kapselointiprotokollia käyttävät VPN-tunnelit, jotka parantavat etähallinnan tietoturvaa huomattavasti. Etähallinta mahdollistetaan ohjelmoitavalle logiikalle eri tavoilla.

Opinnäytetyö onnistui, vaikka VPN-tunneleiden käytössä ilmeni hieman yhteensopivuusongelmia. Antennimittaukset olisi voitu tehdä myös tukiaseman kuuluvuusalueen rajalla, jolloin suunta-antennin merkitys olisi korostunut. Etähallintayhteys saatiin onnistuneesti ohjelmoitavaan logiikkaan.

Avainsanat: 3G, UMTS, HSPA, VPN

Lahti University of Applied Sciences
Degree Programme in Information Technology

NIKANDER, SAKARI: Remote management with 3G-router

Bachelor's Thesis in Telecommunications, 46 pages, 15 appendices

Autumn 2011

ABSTRACT

This Bachelor's thesis was made for DD-Control, a Kouvola-based company, which provides wirelessly and remotely controlled automation solutions for programmable logic controllers. The thesis deals with the enabling and optimization of the 3G (Third Generation) router. Two 3G routers and their suitability for remote management were investigated and compared. Another goal was to investigate the effect of additional antennas on the 3G connection.

3G technology refers to third generation cellular technologies, of which the most commonly used technique in Europe is the UMTS (Universal Mobile Telecommunications System). UMTS uses the broadband code division technique, which enables the theoretical maximum transfer speed of 2 Mbit/s. The UMTS network consists of the core network, radio access network and terminal equipment. Finnish UMTS networks use the 900 and 2100 frequency bands. The first version of the UMTS network has been developed for more efficient use with HSPA (High Speed Packet Access) technology, which allows a theoretical maximum speed of 42 Mbit/s. UMTS network terminals use a variety of different antenna types, which include directional antennas and omni antennas. The most common security features in 3G routers are packet filtering and VPN (Virtual Private Network) support.

When comparing the features of the 3G routers, a clear difference was noticed in the planned uses. The 3G technology used in the devices differs significantly, which affects the equipment deployment. The antenna measurements showed that the use of a directional antenna is not necessary in metropolitan areas. The security features of the 3G routers differ in that they support different VPN technologies. Two different VPN tunnels were formed, and they improved the security of the remote management significantly. Remote management was enabled for the programmable logic controller with different methods.

The Bachelor's thesis was successful, even though there were some compatibility issues in the forming of the VPN tunnels. Antenna measurement could also have been made at the border of the base station coverage area, so the role of the directional antenna would have been more prominent. Remote access connection was successfully formed with the programmable logic controller.

Key words: 3G, UMTS, HSPA, VPN

SISÄLLYS

LYHENNELUETTELO

3G 3rd Generation. Käsittää kolmannen sukupolven matkapuhelinteknologiat.

3GPP Third Generation Partnership Project. Usean standardointijärjestön yhteistyöorganisaatio.

4G 4th Generation. Käsittää neljännen sukupolven matkapuhelinteknologiat.

16-QAM 16-Quadrature Amplitude Modulation. Modulointitekniikka, joka yhdistää vaihe- ja amplitudimodulaation.

AH Authentication Header. Protokolla, joka tarjoaa todennuksen ja takaa viestien eheyden IPSec:ssä.

APN Access Point Name. Operaattorikohtainen liityntäpisteen nimi 3G-yhteydelle.

AuC Authentication Centre. Autentikointikeskus, joka on suojattu tietokanta UMTS-runkoverkossa.

AV Authentication Vector. Autentikointikeskuksen muodostama autentikointivektori.

BCDMA Broadband Code Division Multiple Access. Laajakaistainen koodijakokanavointi, jolla on yli 8 MHz:n kaistanleveys.

CDMA Code Division Multiple Access. Koodijakokanavointi, joka on yksi radiotien kanavanvaraustekniikoista.

CHAP Challenge-Handshake Authentication Protocol. Autentikointiprotokolla, joka perustuu kolmitiekättelyyn.

CK Cipher Key. Salausavain, joka takaa UMTS-verkon luotettavuuden.

CN Core Network. Runkoverkko, joka on tietoliikenneverkon keskeisin osa.

DCH Dedicated transport Channel. UMTS-järjestelmän yhteyskohtainen siirtokanava.

DC-HSPA Dual Carrier High Speed Packet Access. HSPA:n kehittynyt versio, joka käyttää kahta kantoaaltoa.

DC-HSDPA Dual Carrier High Speed Downlink Packet Access. Kahta kantoaaltoa käyttävä HSDPA-tekniikka.

DC-HSUPA Dual Carrier High Speed Uplink Packet Access. Kahta kantoaaltoa käyttävä HSUPA-tekniikka.

DNS Domain Name System. Internetin nimipalvelujärjestelmä, joka muuttaa verkkotunnuksen IP-osoitteeksi.

E-DCH Enhanched Data Channel. Kuljetuskanava, jota käytetään datan siirtoon HSUPA-tekniikassa.

E-DPDCH Enhanched Dedicated Physical Data Channel. Fyysinen kanava, jolla siirretään E-DCH:n data.

EIR Equipment Identity Register. Tietokanta, joka päättää, sallitaanko päätelaitteen käyttäjä UMTS-verkkoon.

ESP Encapsulated Security Protocol. Protokolla, jota käytetään pakettivirtojen salaamiseen IPSec:ssä.

ETSI European Telecommunications Standards Institute. Eurooppalainen telealan standardoimisjärjestö.

EV-DO Evolution Data Optimized. CMDA-2000-tekniikan kehittynyt versio.

FDD Frequency Division Duplex. UMTS:ssa käytettävä taajuusjakoinen tekniikka.

Flash-OFDM Fast Low-latency Access with Seamless Handoff - Orthogonal Frequency Division Multiplexing. OFDM-modulointiin perustuva teknologia, joka on suunniteltu laajakaistakäyttöön.

FPLMTS Future Public Land Mobile Telephony System. UMTS-projektin ensimmäinen työnimi.

GGSN Gateway GPRS Support Node. Internetin ja UMTS-runkoverkon välinen yhdyskäytävä.

GPRS General Packet Radio Service. Pakettikytkentäinen tiedonsiirtopalvelu.

GRE Generic Routing Encapsulation. Ciscon kehittämä IP-tunnelointiprotokolla.

GSM Global System for Mobile Communications. Maailmanlaajuinen matkapuhelinjärjestelmä.

HLR Home Location Register. Tietokanta, jossa on kaikki hallinnollinen tieto käyttäjistä ja käyttäjien viimeisin tiedetty sijainti.

HSPA High Speed Packet Access. Kahden matkaviestintekniikan yhdistelmä, joka parantaa olemassa olevan UMTS-tekniikan siirtonopeutta.

HS-DSCH High Speed Downlink Shared Channel. Datan siirrolle tarkoitettu kanava HSDPA:ssa.

HSDPA High Speed Downlink Packet Access. Matkaviestinten yhteyskäytäntö, joka kasvattaa UMTS-verkon alavirran siirtonopeutta.

HSUPA High Speed Uplink Packet Access. UMTS-verkon ylävirran siirtonopeutta kasvattava tekniikka.

IK Integrity Key. Salausavain, jolla tarkistetaan tiedon eheys UMTS-verkossa.

IKE Internet Key Exchange. Turvallisen kommunikaatiokanavan tarjoava kaksisuuntainen protokolla.

IMEI International Mobile Equipment Identity. Päätelaitteen laitetunnus.

IMSI International Mobile Subscriber Identity. Tilaajatunnus, jolla suojataan UMTS-verkon käyttäjätiedot.

IMT-2000 International Mobile Telecommunication 2000. ITU:n määrittelemä standardiryhmä.

I/O Input / Output. Kahden järjestelmän välinen liitäntä.

IP Internet Protocol. Protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa.

IPSec Internet Protocol Security. Verkkokerroksella toimiva VPN-kapselointiprotokolla.

ISAKMP Internet Security Association Key Managemenet Protocol. Protokolla, joka kuvaa IPSec-yhteyden neuvotteluvaiheen.

ITU International Telecommunications Union. Televiestintäverkkoja ja -palveluja kansainvälisesti koordinoiva järjestö.

ITU-R ITU Radiocommunication Sector. ITU:n radioviestintäsektori.

LAC Location Are Code. 3G-verkon aluekoodi.

LTE Long Term Evolution. UMTS-teknologiapuun 4G-tekniikka.

MAC Media Access Control. Verkkosovittimen ethernet-verkossa yksilöivä osoite.

MAC Message Authentication Code. Todennusluku, jonka avulla UMTS-verkko autentikoidaan päätelaitteelle.

MCC Mobile Country Code. UMTS-verkon maakohtainen koodi.

MGW Multimedia Gateway. Yhdyskäytävä UMTS-runkoverkossa.

MIMO Multiple Input Multiple Output. Tekniikka, jossa käytetään useaa vastaanotto- ja lähetysantennia.

MISO Multiple Input Single Output. Tekniikka, jossa käytetään useaa lähetysantennia ja yhtä vastaanottoantennia.

MNC Mobile Network Code. Operaattorikohtainen koodi UMTS-verkossa.

MPPE Microsoft Point-to-Point Encryption. Microsoftin kehittämä salausprotokolla.

MS Mobile Station. GSM-verkon päätelaite.

MS_CHAPv2 Microsoft Challenge-Handshake Protocol version 2. Microsoftin versio CHAP-autentikointiprotokollasta.

MSC Mobile Switching Centre. UMTS-runkoverkon piirikytkentäinen matkapuhelinkeskus.

OSI Open Systems Interconnection. Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.

PAP Password Authentication Protocol. Salasanaa käyttävä autentikointiprotokolla.

PIN Personal Identification Number. Koodi, jolla autentikoidaan USIM-kortti.

PPP Point-to-Point Protocol. Protokolla, jolla muodostetaan yhteys verkkolaitteiden välillä.

PPTP Point-to-Point Tunneling Protocol. PPP-protokollaan perustuva VPN-tunnelointiprotokolla.

QoS Quality of Service. Termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia.

QPSK Quadrature Phase Shift Keying. Neljää kantoaallon vaihetta käyttävä nelivaiheinen vaiheavainnus.

RNC Radio Network Controller. UMTS-verkkoa hallitseva elementti, joka ohjaa tukiasemia.

RNS Radio Network System. UMTS-verkon osa, johon kuuluu RNC ja tukiasemat.

RSSI Received Signal Strength Indicator. Vastaanotettu signaalinvoimakkuus.

SGSN Serving GPRS Support Node. UMTS-runkoverkon pakettikytkentäinen elementti.

SIM Subscriber Identity Module. Käyttäjäkohtainen matkapuhelinliittymän älykortti.

SIMO Single Input Multiple Output. Tekniikka, jossa käytetään yhtä lähetysantennia ja useita vastaanottoantenneja.

SMA SubMiniature version A. Antennien koaksaalikaapeleissa käytetty liitin.

SMS Short Message Service. Tekstiviesti.

SNMP Simple Network Management Protocol. TCP/IP-verkkojen hallinnassa käytettävä protokolla.

TCP/IP Transmission Control Protocol / Internet Protocol. Usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.

TD-CDMA Time Division-Code Division Multiple Access. Aika- ja koodijako-kanavoinnin yhdistävä tekniikka.

TDD Time Division Duplex. UMTS:ssa käytettävä aikajakoinen tekniikka.

TMSI Temporary Mobile Subscriber Identity. Tilapäinen tunniste joka suojaa IMSI:n

UE User Equipment. UMTS-verkon päätelaite.

UICC UMTS Integrated Circuit Card. Integroitu piiri, jolle USIM sijoitetaan.

UMTS Universal Mobile Telecommunications System. Kolmannen sukupolven matkapuhelinteknologia.

URL Uniform Resource Locator. Merkkijono, joka osoittaa Internet-sivuston.

USB Universal Serial Bus. Sarjaväyläliitin.

USIM Universal Subscriber Identity Module. Käyttäjäkohtainen matkapuhelinliittymän älykortti UMTS-järjestelmässä.

UTRA Universal Terrestrial Radio Access. UMTS-järjestelmän radioverkon pääsy.

UTRAN Universal Terrestrial Radio Access Network. UMTS radioliityntäverkko.

VOIP Voice Over Internet Protocol. Tekniikka, jolla voidaan siirtää ääntä reaaliaikaisesti IP-protokollaa käyttävän verkon välityksellä.

VLR Visitor Location Register. Tilapäinen rekisteri, jonne tallennetaan sen alaisuudessa olevien tilaajien tietoja.

VPN Virtual Private Network. Internetin yli muodostettava virtuaalinen yksityinen verkko.

WAN Wide Area Network. Lähiverkot yhdistävä laajaverkko kuten Internet.

WCDMA Wideband Code Division Multiple Access. UMTS-verkossa käytettävä laajakaistainen koodijakokanavointitekniikka.

WLAN Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Matkapuhelintekniikoiden kehittyessä keskitytään yhä enemmän laajakaistaisiin langattomiin ratkaisuihin etähallinnassa. Tämä opinnäytetyö tehdään Kouvolassa toimivalle DD-Control-yritykselle, joka tarjoaa langattomasti etähallittavia automaatioratkaisuja ohjelmoitaviin logiikoihin. Monet yrityksen tarjoamat etähallintaratkaisut toimivat kuitenkin suljetussa radiomodeemiverkossa, joka ei sovi kaikille ratkaisuille. Vaihtoehtoisesti automaation etähallinta toteutetaan 3G-tekniikalla (Third Generation) Internetin välityksellä, jolloin tietoturvalla on yhä suurempi merkitys.

Tämä opinnäytetyö käsittelee langattoman etähallinnan mahdollistamista ja optimointia 3G-reitittimellä. Opinnäytetyössä tutkitaan ja vertaillaan kahta 3G-reititintä ja niiden soveltuvuutta etähallintaan. Tavoitteena on myös tutkia lisäantennien vaikutusta muodostettavaan 3G-yhteyteen. Opinnäytetyön tutkimusongelmana on ottaa selvää, miten 3G-reititin ja mahdollinen tietoturva otetaan käyttöön etähallintaratkaisuun ja miten käytettävä lisäantenni vaikuttaa etähallintaan.

Opinnäytetyössä tutkittava 3G-tekniikka rajataan UMTS-teknologiapuun (Universal Mobile Telecommunications System) tekniikoihin. Työssä kerrotaan lyhyesti 3G-antennityypeistä ja antennin asennuksesta. 3G-reitittimien tietoturvassa keskitytään pakettisuodattavaan palomuuritekniikkaan ja VPN-tunneleihin (Virtual Private Network). Työssä käytetään enimmäkseen erilaisia 3G-tekniikan Internetlähteitä sekä jonkin verran aiheeseen liittyviä kirjallisuuslähteitä.

2 KOLMANNEN SUKUPOLVEN TEKNIIKAT

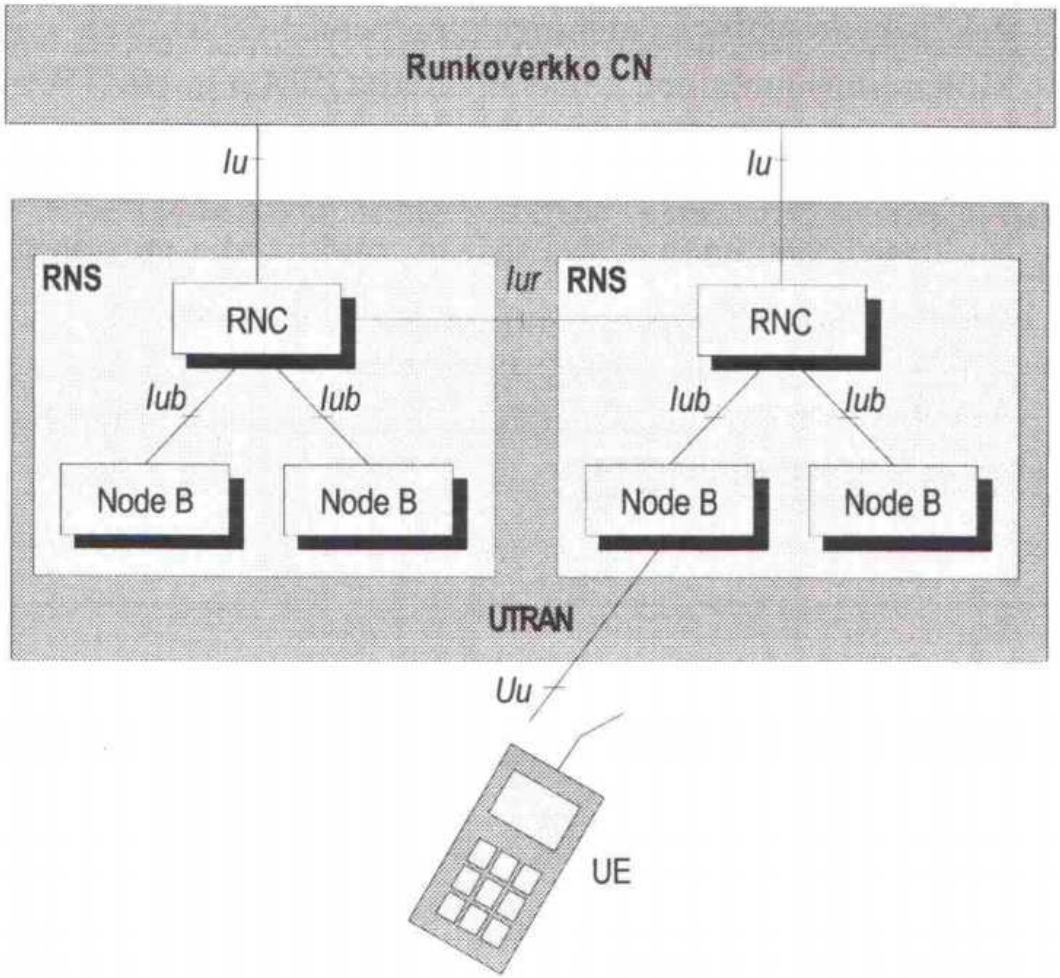
2.1 UMTS

Matkapuhelintekniikassa, kolmannen sukupolven tekniikalla tarkoitetaan yleisesti UMTS-tekniikkaa, kun puhutaan 3G-tekniikasta Euroopassa. UMTS-tekniikan on kehittänyt 3GPP (Third Generation Partnership Project), ja UMTS kuuluu ITU:n (International Telecommunications Union) määrittelemään IMT-2000 (International Mobile Telecommunication 2000)-standardiryhmään. UMTS-projekti alkoi työnimellä FPLMTS (Future Public Land Mobile Telephony System), ja sen tarkoituksena oli laatia ratkaisumalleja kolmannen sukupolven puhelinjärjestelmää varten. Projekti nimettiin myöhemmin uudelleen IMT-2000:ksi, ja ratkaisumalleista päädyttiin hyödyntämään pääasiassa WCDMA- (Wideband Code Division Multiple Access) ja CDMA2000-tekniikoita (Code Division Multiple Access 2000). CDMA2000-tekniikkaa käytetään mm. Yhdysvalloissa ja Japanissa, kun taas WCDMA-tekniikkaa käyttävä UMTS on yleinen Euroopassa. UMTS-verkon palvelukirjoista poimittuja tavoitteita ovat mm. kiinteän verkon tasoinen äänenlaatu, 144 kbit/s – 2 Mbit/s siirtonopeus laitteen liikkuvuudesta riippuen, radiokaistan mahdollisimman tehokas käyttö sekä tuki piiri- ja pakettikytkentäiselle tiedonsiirrolle. (Granlund 2007, 417.)

UMTS:sta on tullut eniten käytetty 3G-järjestelmä kaikista IMT-2000-standardiryhmän järjestelmistä. UMTS-järjestelmän käyttö aloitettiin Euroopassa, mutta UMTS on levinnyt nopeasti ympäri maailmaa. UMTS tarjoaa globaalin verkkovierailun, ja UMTS on suunniteltu mahdollistamaan useampia sovelluksia kuin monet sen kilpailijat. UMTS myös perustuu onnistuneeseen GSM-standardiin (Global System for Mobile Communications), jonka kanssa UMTS on yhteensopiva. Tämä antoi UMTS:lle laajan pohjan, jolle rakentaa. Ensimmäinen UMTS-standardin versio julkaistiin vuonna 1999, ja version nimeksi annettiin release 99. Ensimmäiset kaupalliset UMTS-verkot tulivat kuitenkin vasta vuoden 2001 jälkeen. (UMTS 3G History 2001.)

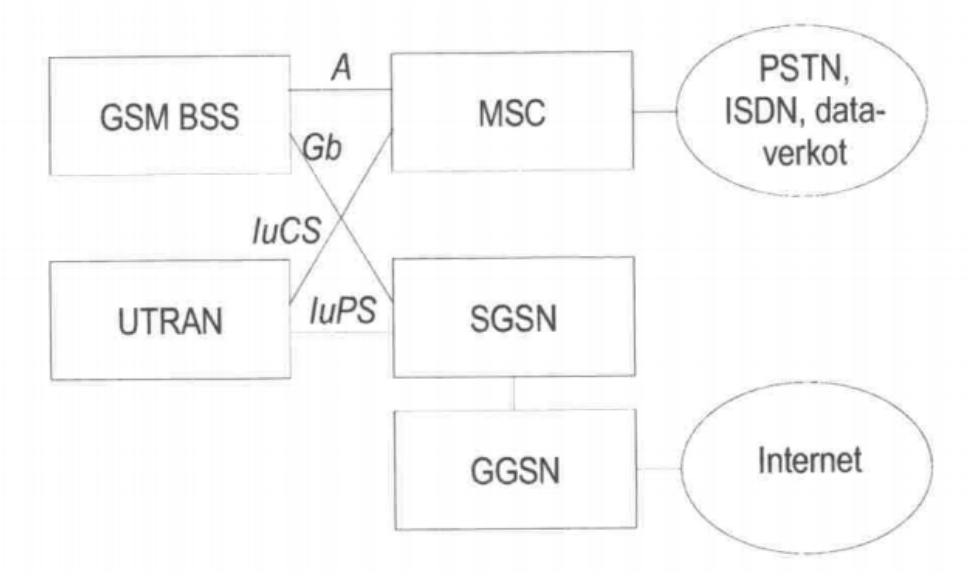
2.1.1 UMTS-verkon arkkitehtuuri

UMTS-verkko voidaan jakaa kolmeen osaan, joita ovat runkoverkko CN (Core Network), UMTS radioliityntäverkko UTRAN (Universal Terrestrial Radio Access Network) ja käyttäjän päätelaitteet UE (User Equipment). Verkon osat yhdistetään erilaisilla rajapinnoilla. CN ja UTRAN yhdistetään lu-rajapinnalla, kun taas UTRAN ja UE yhdistetään radiorajapinnalla Uu. CN ja UTRAN voidaan myös jakaa pienempiin osiin. UTRAN koostuu radioverkko-ohjaimista RNC (Radio Network Controller) ja niiden tukiasemista, joita kutsutaan nimellä NODE B. RNC ja tukiasemat ovat yhteydessä toisiinsa lub-rajapinnalla ja muodostavat radiojärjestelmän RNS (Radio Network System). RNS:t puolestaan yhdistetään lur-rajapinnalla. Kuviosta 1 nähdään koko UMTS-verkon rakenne, jossa on myös osoitettu UTRAN:n osat. (Penttinen 2006, 64 – 65.)



KUVIO 1. UMTS-verkon rakenne (Penttinen 2006, 65)

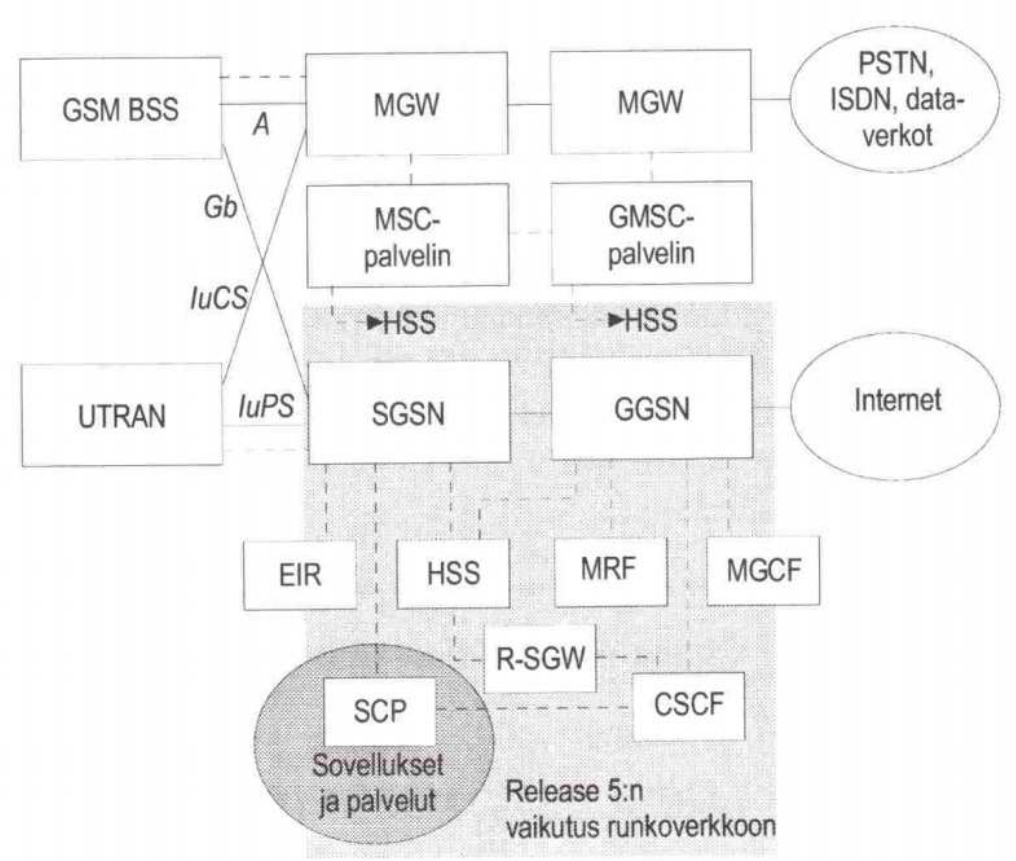
Runkoverkon rakenne määräytyy UMTS-verkon käyttämän spesifikaatioiden mukaan. UMTS-verkon perusversio on 3GPP:n vuonna 2000 julkaisema release 99. Release 99:llä määritellään ensimmäinen UMTS-verkko, joka kehittyy käyttöönoton jälkeen release 4:n, release 5:n ja uudempien versioiden mukaisilla verkkomäärityksillä. Runkoverkon ensimmäisen vaiheen on sisällettävä GSM-release 99:n määrittelemät verkkomääritykset, minkä jälkeen runkoverkkoa päivitetään release 4:n ja uudempien määritysten mukaiseksi. Vaikka UMTS-järjestelmän radioverkko on täysin erilainen kuin GSM-järjestelmässä, voidaan UMTS-järjestelmän runkoverkon resursseja jakaa GSM- ja GPRS-järjestelmien (General Packet Radio Service) kesken. GSM:n tukiasemajärjestelmä BSS (Base Station Sub-system) voidaan liittää UMTS-järjestelmän runkoverkkoon A- tai Gb-rajapinnoilla, joista A-rajapinnalla yhdistetään GSM:n piirikytkentäiset palvelut ja Gb-rajapinnalla yhdistetään GPRS:n pakettikytkentäiset palvelut. Kuviossa 2 näkyy Release 99:n mukainen UMTS-runkoverkko, jossa osoitetaan myös GSM-yhteensopivuus rajapinnoilla A ja Gb. (Penttinen 2006, 65 - 66.)



KUVIO 2. UMTS-järjestelmän release 99 mukainen runkoverkko (Penttinen 2006, 66)

Kuviosta 2 nähdään, kuinka runkoverkko koostuu kahdesta alueesta, jotka ovat piiri- ja pakettikytkentäiset elementit. Kuvion 2 piirikytkentäisiin elementteihin kuuluu ainoastaan matkapuhelinkeskus MSC (Mobile Switching Centre), kun taas release 4:n ja uudempien määritysten mukaisissa runkoverkoissa piirikytkentäisiä

elementtejä on enemmän. Piirikytkentäisien elementtien tehtävänä on kuljettaa dataa piirikytkentäisesti, esimerkiksi muodostamalla kanava puhelun ajaksi. Pakettikytkentäiset elementit puolestaan kuljettavat dataa paketteina, mikä mahdollistaa tehokkaamman verkon käytön kapasiteettia jakamalla. Kuvion 2 pakettikytkentäiset elementit ovat SGSN (Serving GPRS Support Node) ja GGSN (Gateway GPRS Support Node). SGSN:n tehtäviin kuuluu liikkuvuuden hallinta, istunnon hallinta, kommunikointi muiden runkoverkon alueiden kanssa ja laskutus. GGSN:n tehtävänä on toimia yhdyskäytävänä Internetin ja runkoverkon välissä sekä reitittää tuleva data UMTS-verkon käyttäjille. Piiri- ja pakettikytkentäisillä elementeillä on myös jaettuja elementtejä, joita kuviossa 2 ei näytetä. Näitä jaettuja elementtejä ovat HLR (Home Location Register), EIR (Equipment Identity register) ja AuC (Authentication Centre). HLR on tietokanta, jossa on kaikki hallinnollinen tieto käyttäjistä ja käyttäjien viimeisin tiedetty sijainti. Tällä tavoin HLR osaa reitittää puhelut halutulle RNC:lle ja tukiasemalle. EIR-tietokanta päättää sallitaanko päätelaitteen käyttäjä verkkoon. Jokaisella UE:lla on IMEI-tunnus (International Mobile Equipment Identity), jonka EIR tarkistaa. AuC on suojattu tietokanta, jossa on salainen avain K, joka löytyy myös käyttäjän USIM-kortista (Universal Subscriber Identity Module). (UMTS / WCDMA Network Architecture 2011.)



KUVIO 3. Release 5:n määritysten mukainen UMTS-runkoverkko (Penttinen 2006, 68)

Kuviosta 3 nähdään, kuinka UMTS-runkoverkko muuttuu release 99:n määritysten mukaisesta runkoverkosta uudemman release 5:n määritysten mukaiseksi. Huomataan, että piirikytkentäinen MSC on muuttunut MSC-palvelimiin ja MGW-elementteihin (Multimedia Gateway). MSC:n muutos tapahtui release 4:n määrityksissä, kun taas pakettikytkentäisten SGSN:n ja GGSN:n muutokset tulivat release 5:n myötä. (Penttinen 2006, 69.)

GSM-järjestelmästä poiketen UMTS-verkon päätelaitteen nimitys on muutettu UE:ksi, mikä laajentaa päätelaitteen käyttöaluetta liikkuvasta asemasta MS (Mobile Station) laitteeseen, joka kykenee liittymään UMTS-verkkoon rajoittamatta päätelaitteen käytettävyyttä millään tavalla. ETSI:n (European Telecommunications Standards Institute) suositus TR 121 904 kuvaa UMTS-päätelaitteen toimintoja, joita ovat mm. lyhytsanomapalvelu, hätäpuhelut, puheen siirto, solukohtaisten levitysviestien käsittely, UMTS-verkon lisäpalvelujen tuki, sijaintipalvelut, GSM-verkon palvelut ja paketti- sekä piirikytkentäisen datan siirto. Myös SIM-

kortista (Subscriber Identity Module) käytetään UMTS-järjestelmässä erilaista nimitystä, joka on USIM. USIM sijoitetaan integroidulle piirille, joka on nimeltään UICC (UMTS Integrated Circuit Card). Hätäkutsuja lukuunottamatta USIM-kortin on oltava päätelaitteessa, jotta sitä voidaan käyttää. Tällä tavoin puhelimen sisältämä UMTS-päätelaite toimii kuten GSM-puhelin. USIM-kortin tehtävä on yksilöidä käyttäjä ja sille tallennetaan tietoturvalle olennaiset osat, kuten liittymäkohtainen salainen avain K ja algoritmit. USIM-kortin autentikointi perustuu SIM-kortin tavoin PIN-koodiin (Personal Identification Number). USIM PIN-koodin pituus on 4 - 8 merkkiä ja sen lisäksi on olemassa 8-merkkinen unblock PIN, jota ei käyttäjän toimesta voi muuttaa. Unblock PIN -koodilla voidaan palauttaa USIM-kortti käyttöön, jos sille on syötetty virheellinen PIN-koodi kolme kertaa. (Granlund 2007, 418 - 419.)

UE:lla on kolme toimintatilaa, jotka ovat piirikytkentäinen tila CS (Circuit Switched), pakettikytkentäinen tila PS (Packet Switched) ja niiden yhdistelmätila PS/CS. CS-tilassa päätelaite pystyy vain käyttämään piirikytkentäisiä palveluita, kun taas PS-tilassa päätelaite pystyy käyttämään pakettikytkentäisiä palveluita. PS-tilassa voidaan myös käyttää piirikytkentäisiä palveluita, kuten VOIP (Voice Over Internet Protocol). PS/CS-tilassa voidaan puolestaan käyttää sekä piiri- että pakettikytkentäisiä palveluita. Kuviossa 3 nähdään runkoverkon paketti- ja piirikytkentäiset luCS- ja luPS-rajapinnat. (UMTS Overview 2002.)

2.1.2 UMTS-verkon tekniikka

UTRA (Universal Terrestrial Radio Access) eli UMTS-järjestelmän radioverkon pääsy jaetaan kahteen komponenttiin, jotka ovat aikajakoinen TDD-tekniikka (Time Division Duplex) ja taajuusjakoinen FDD-tekniikka (Frequency Division Duplex). UTRA:n FDD-komponentti toteutetaan WCDMA:lla eli laajakaistaisella koodijakotekniikalla. TDD-komponentti puolestaan toteutetaan TD-CDMA-tekniikalla (Time Division CDMA), joka on CDMA- (Code Division Multiple Access) ja TDMA-tekniikoiden (Time Division Multiple Access) yhdistelmä. WCDMA on määritelty käytettäväksi FDD-alueelle, joka on parillinen taajuusalue. Spesifikaatioiden mukaan parillisia taajuusalueita ovat 1920 – 1980 MHz

ylävirtaan ja 2110 – 2170 MHz alavirtaan. Näitä taajuusalueita kutsutaan UMTS 2100 -taajuuskaistaksi. TD-CDMA käyttää paritonta taajuusaluetta eli TDD-aluetta, joka voi teoriassa olla mikä tahansa, jos käytettävissä on vähintään 3,84 MHz:n kaistanleveys 200 kHz:n kanavajaottelulla. Kuviosta 3 nähdään Suomen viestintäviraston myöntämät operaattorien UMTS-taajuudet TDD- ja FDD-tyypeillä. (Penttinen 2006, 69.)

TAULUKKO 1. Suomen UMTS-taajuudet (Radiolupapäätös 18305/730/2006 2006; Radiolupapäätös 228/702/2009 2009; Radiolupapäätös 12979/730/2009 2009)

	Tyyppi	Taajuus ylävirtaan (MHz)	Taajuus alavirtaan (MHz)
TeliaSonera Finland Oyj	TDD (keskitaajuus)	1902,4	
	FDD	1959,9 – 1979,7	2149,9 – 2169,7
Elisa Oyj	TDD (keskitaajuus)	1917,4	
	FDD	1920,3 – 1940,1	2110,3 – 2130,1
DNA Finland Oy	TDD (keskitaajuus)	1907,4	
	FDD	1940,1 – 1959,9	2130,1 – 2149,9
Ålands Mobiltelefon Ab	TDD (keskitaajuus)	1917,4	
	FDD	1920,3 – 1935,3	2110,3 – 2125,3

3GPP:n teknisessä spesifikaatiossa 25.101 on myös määritelty muita käytettäviä UTRA FDD -taajuusalueita, jotka eivät kuitenkaan ole niin suuressa käytössä kuin edellä mainittu UMTS 2100 -taajuuskaista. Toinen mahdollinen UTRA FDD -taajuuskaista on UMTS 900, joka käyttää parillisia taajuusalueita, jotka ovat 880 – 915 MHz ylävirtaan ja 925 – 960 MHz alavirtaan. Kyseinen UMTS 900 -taajuuskaista on suosittu mm. Suomessa, koska voidaan käyttää valmiiksi rakennettuja 900 MHz GSM-verkon mastopaikkoja ja UMTS 900:lla on pidempi signaalin kantomatka. (3GPP TS 25.101 2011.)

WCDMA perustuu CDMA-tekniikkaan, joka voidaan jakaa CDMA-, WCDMA- ja BCDMA-tekniikkoihin (Broadband Code Division Multiple Access). CDMA-tekniikat eroavat kaistanleveyksillään, jotka ovat noin 1 MHz CDMA:lle, vähintään 5 MHz WCDMA:lle ja yli 8 MHz BCDMA:lle. WCDMA-tekniikka tuo UMTS-verkolle ominaisuuksia, jotka erottavat sen toisen sukupolven tekniikoista.

Kyseisiä ominaisuuksia ovat mm. joustava tiedonsiirtokapasiteetti, parempi taajuuksien uudelleenkäyttö ja teoreettinen 2 Mbit/s siirtonopeus. (Granlund 2007, 422.)

UMTS-järjestelmän kanavat voivat olla loogisia, fyysisiä tai siirtokanavia. Menetelmä eroaa GSM-järjestelmästä siten, että UMTS:ssä voidaan kuljettaa yhtä tai useampaa siirtokanavaa useilla eri tyyppisillä fyysisillä kanavilla, kun taas GSM:ssä yhdellä fyysisellä kanavalla voi olla yksi tai useampi looginen kanava. Kanavilla on omat tehtävänsä. Fyysiset kanavat vastaavat siitä, minne data siirretään. Siirtokanavat vastaavat siitä, miten data siirretään. Loogiset kanavat vastaavat, mitä siirretään. UTRA-FDD:ssä loogiset kanavat jaetaan osoittimiin ja siirtokanaviin. Siirtokanavat puolestaan jaetaan yhteyskohtaisiin ja yhteisiin kanaviin. UMTS-järjestelmässä on vain yksi yhteyskohtainen siirtokanava DCH (Dedicated transport Channel), kun taas osoittimia ja yhteisiä kanavia on useita. Fyysiset kanavat jaetaan ylä- ja alavirtakanaviin. (Penttinen 2006, 74 - 75.)

2.1.3 UMTS-verkon tietoturva ja autentikointi

UMTS- ja GSM-verkot käyttävät samantapaista käyttäjätietojen suojausta ja autentikointia. UMTS-verkon käyttäjätiedot suojataan GSM-verkon tapaisella tilaajatunnisteella IMSI (International Mobile Subscriber Identity), joka puolestaan suojataan tilapäisellä tunnisteella TMSI (Temporary Mobile Subscriber Identity). Tällöin liittymän tiedot eivät ole luvattomassa käytössä. Verkko ei voi esimerkiksi paljastaa käyttäjän laitteen sijaintia, eikä salakuuntelemalla voida paljastaa käyttäjälle tarjottuja palveluita. (Granlund 2007, 419.)

UMTS-verkon autentikaatiolla tarkoitetaan tilaajaliittymän varmennusta siihen valtuutettuun USIM-korttiin ja laitteeseen. UMTS-päätelaite voi myös autentikoida verkon, mikä ei ole mahdollista GSM-verkossa. Jotta saavutettaisiin riittävä turvallisuus, autentikointi tapahtuu aina yhteyden muodostuessa verkon ja laitteen välille. Autentikointi ei siis tapahdu ainoastaan kytkeytymisen yhteydessä, kun käyttäjä autentikoituu USIM-kortille PIN-koodilla, vaan myös palvelupyynnön ja sijainnin päivityksen yhteydessä. (Granlund 2007, 419.)

Autentikoinnissa on useita vaiheita. Aluksi laite pyytää autentikointikeskukselta AuC auntentikointivektorin AV (Authentication Vector), kun kirjaudutaan verkkoon tai uuden vierailijarekisterin VLR (Visitor Location Register) alaisuuteen. VLR on tilapäinen rekisteri, jonne tallennetaan sen alaisuudessa olevien tilaajien tietoja. VLR vastaanottaa AuC:lta vektorin, joka on 5-sarakkeinen taulukko, jossa on tietty määrä rivejä. Sarakkeet ovat satunnaisluku RAND, RAND:sta laskettu vastaus XRES, autentikointikoodi AUTN ja salausavaimet CK (Cipher Key) sekä IK (Integrity Key). Jokainen rivi on voimassa yhden autentikointikerran, jonka jälkeen poistetaan käytetty rivi. VLR tallentaa seuraavaksi AV:n ja lähettää AUTN:n ja RAND:n päätelaitteelle. Päätelaite vertaa AUTN:a koodiin, joka on USIM-kortissa ja laskee satunnaisluvusta RAND vastauksen RES. Päätelaite saa myös AUTN:sta MAC-koodin (Message Authentication Code), jonka avulla verkko autentikoidaan päätelaitteelle. Päätelaite laskee RAND:n ja kahden muun AUTN:sta saadun arvon perusteella XMAC:n, jota verrataan UMTS-verkolta saatuun MAC-koodiin. Jos MAC- ja XMAC-koodit täsmäävät, verkko on todennut itsensä päätelaitteelle. RES palauteteaan VLR:ään, joka vertaa sitä vektorissa olevaan XRES:iin. Laite hyväksytään verkon puolelta, jos vastaukset täsmäävät. Lopuksi VLR ottaa käyttöön lähetetyn RAND-luvun rivin salausavaimet CK ja IK. Päätelaite puolestaan muodostaa vastaanotetun RAND-luvun avulla samat salausavaimet. (Granlund 2007, 419 - 420.)

AV:n loput rivit käytetään seuraavilla laitteen autentikointikerroilla, ja rivien loppuessa koko autentikointiprosessi aloitetaan uudestaan. Autentikointimenetelmä varmistaa, että laskennassa käytetyt avaimet eivät päädy operaattorin tai USIM-kortin ulkopuolelle, sillä kaikki laskenta tapahtuu joko USIM-kortilla tai AuC:ssa. Laskennassa käytetään viittä eri algoritmia, joita kutsutaan algoritmeiksi f1 – f5. UMTS-verkon luottamuksellisuus taataan käyttämällä autentikoinnissa luotua avainta CK, ja käyttämällä salakirjoitusta. Salakirjoitus muodostetaan jonosalaajalla, joka käyttää algoritmia f8. Autentikoinnin ja salakirjoituksen lisäksi tiedon eheys tarkistetaan avaimella IK. Lähetettävän sanoman perään liitetään siis algoritmilla f9 muodostettu tarkiste, jota vastaanottaja vertaa omalla IK-avaimella muodostettuun tarkasteeseen. (Granlund 2007, 420 - 421.)

2.2 HSPA

3G-tekniikoiden kehittyessä on UMTS-verkolle syntynyt uusia, aiempaa nopeampia datapalveluita. Nämä datapalvelut ovat nimeltään HSDPA (High Speed Downlink Packet Access) ja HSUPA (High Speed Uplink Packet Access), joiden yhteisnimitys on HSPA (High Speed Packet Access). HSPA on siis kahden matkaviestintekniikan yhdistelmä, joka parantaa olemassa olevan UMTS-tekniikan siirtonopeutta. Alkuperäinen UMTS-standardi mahdollisti 384 kbit/s maksimilatausnopeuden. Tarvittiin kuitenkin paljon suurempi siirtonopeus, jotta voitaisiin kilpailla kiinteiden laajakaistapalveluiden kanssa. Tämä johti 3G HSPA-tekniikan kehitykseen. (HSPA Tutorial 2011.)

Release 99:n määritysten mukainen UMTS-verkko oli suuntautunut enemmän kohti piirikytkettyä toimintaa, joten release 99 ei soveltunut kovin hyvin HSPA-tekniikan vaatimaan pakettikytkentäiseen toimintaan. HSPA-tekniikan vaatimat muutokset sisällytettiin moniin UMTS-verkkoihin, jotta päästäisiin halutun HSPA:n tarjoaman siirtonopeuden tasolle. Nopeampi siirtonopeus ei ole kuitenkaan ainoa HSPA-tekniikan tuoma etu. Muita etuja ovat mm. korkeamman luokan modulaatio, lyhyempi aikajakso TTI (Transmission Time Interval) ja kanavan jako. (HSPA Tutorial 2011.)

2.2.1 HSDPA

HSDPA on 3GPP:n release 5 -versiossa tullut paranneltu yhteyskäytäntö UMTS-järjestelmälle. HSDPA tarjoaa paljon suuremman siirtonopeuden alavirtaan eli tukiasemasta päätelaitteeseen. Alavirtaan siirrettiin paljon enemmän tietoa verrattuna ylävirtaan, joten latausnopeuden kehittäminen oli etusijalla. HSDPA toi useita muutoksia 3GPP:n perus-UMTS-standardiin nähden. Alunperin WCDMA-tekniikka käytti vain QPSK-modulointia (Quadrature Phase Shift Keying), joka on neljää kantoaallon vaihetta käyttävä nelivaiheinen vaiheavainnus. QPSK käyttää siis neljää tilaa per symboli eli voidaan ilmaista 2 bittiä. HSDPA puolestaan voi käyttää alavirtaan 16-QAM-modulointia (16-Quadrature Amplitude Modulation), joka on vaihe- ja amplitudimodulaation yhdistävä modulointitekniikka. 16-QAM-

modulaatio käyttää 16 tilaa per symboli, joten siirrettävien bittien lukumäärä per symboli on 4. 16-QAM on siis kaksi kertaa nopeampi kuin QPSK. (Granlund 2007, 430 - 431.)

16-QAM-modulaatiolla on kuitenkin heikompi vastustuskyky melulle, joten ennen lähetystä on otettava selvää yhteyden vahvuudesta. Yhteyden sopivuudesta otetaan selvää analysoimalla erilaisia parametrejä, kuten fyysisen kerroksen olosuhteet, tehonsäätö, QoS (Quality of Service) ja HSDPA:n ominaiset tiedot. Toinen olennainen muutos on HARQ-toipumisen (Hybrid Automatic Repeat Request) käyttöönotto, jolla vältetään langattoman TCP-liikenteen ongelmia. Tämä tarkoittaa sitä, että negatiivinen ja positiivinen kuittaus palautetaan lähettäjälle 10 ms:n sisällä virheellisen sanoman saapumisesta. Kuittauksen käsittely on siis siirretty verkosta tukiasemalle Node B. (HSDPA Tutorial 2011.)

HSDPA toi lisää kanavia, jotta voitaisiin kuljettaa dataa halutulla tavalla ja annettaisiin lisää reagointikykyä järjestelmälle. Datan siirrolle tarkoitettu kanava HS-DSCH (High Speed Downlink Shared Channel) on myös jaettu eli käyttäjien data siirtyy samalla aikajakokanavoidulla kanavalla. HS-DSCH-kanavan tiedot siirretään fyysisellä kanavalla HS-DPSCH (High Speed Dedicated Physical Shared Channel). Järjestelmän reagointikykyä parannettiin lyhentämällä aikaväliä TTI. Release 99:n määritysten mukainen 10-80 ms:n TTI lyhennettiin 2 ms:iin. Lyhyempi TTI vaati myös nopeampaa dataliikenteen ohjausta. Jokainen 2 ms:n aikaväli voidaan levittää SF-16-hajautusavaimella 15 rinnakkaiseksi kanavaksi. Jokainen aikaväli voi siis kuljettaa 2 ms:n aikana 15 eri käyttäjän dataa, tai yhden käyttäjän dataa, joka on hajautettu 15 osaan. Taulukossa 2 on luokiteltu HSDPA:n suorituskyky eri luokkiin koodauksen, moduloinnin ja rinnakkaisten kanavien lukumäärän mukaan. Taulukon huippunopeudet ovat kuitenkin vain teoreettisia, ja käyttännön siirtonopeus on riippuvainen esimerkiksi päätelaitteesta ja radiotien olosuhteista. (Granlund 2007, 431 – 433.)

TAULUKKO 2. HSDPA suorituskykyluokat (Granlund 2007, 432)

HS-DSCH-luokka	SF-16 kanavien lukumäärä	TTI-väli	Modulointi	Huippunopeus Mbit/s
Category 1	5	3	QPSK & 16-QAM	1,2
Category 2	5	3	QPSK & 16-QAM	1,2
Category 3	5	2	QPSK & 16-QAM	1,8
Category 4	5	2	QPSK & 16-QAM	1,8
Category 5	5	1	QPSK & 16-QAM	3,6
Category 6	5	1	QPSK & 16-QAM	3,6
Category 7	10	1	QPSK & 16-QAM	7,3
Category 8	10	1	QPSK & 16-QAM	7,3
Category 9	15	1	QPSK & 16-QAM	10,2
Category 10	15	1	QPSK & 16-QAM	14,4
Category 11	5	2	QPSK	0,9
Category 12	5	1	QPSK	1,8

2.2.2 HSUPA

HSUPA on 3GPP:n kehittämä HSDPA:ta vastaava tekniikka, joka otettiin käyttöön versiossa release 6. HSUPA on kehitetty ylävirran siirtonopeuden nostamiseen ja latenssin laskemiseen. HSUPA käyttää samantyyppisiä ratkaisuja kuin HSDPA, jotta se saavuttaa korkeamman siirtonopeuden. Pääasiassa HSUPA eroaa HSDPA:sta moduloinnissa. HSUPA:ssa käytetään BPSK-modulointia (Binary Phase Shift Keying), joka on kahden vaihe-eron binäärinen vaiheavainnus. Sillä voidaan siis ilmaista vain 1 bitti. Korkeamman luokan 64-QAM-modulaatio otettiin myös käyttöön release 7:ssä. 64-QAM-modulaatiolla voidaan puolestaan ilmaista 6 bittiä. HSUPA:n ja HSDPA:n yhteisiä ominaisuuksia ovat mm. HARQ, nopeampi dataliikenteen ohjaus ja lyhyempi TTI. (HSUPA Tutorial 2011.)

HSDPA:n tavoin tietoliikenteen hallinta on tukiaseman tehtävä HSUPA:ssa. HSUPA kuitenkin eroaa HSDPA:sta siten, että HSDPA on vapaa ohjaamaan verkon päätelaitteille siirtyvää dataa, jolloin siirtotien kapasiteetti voidaan käyttää statistisen aikajakokanavoinnin periaatteella. HSUPA:ssa puolestaan päätelaite saa

itselleen hajautusavaimeen perustuvan omistetun datakanavan, jolla liikennöidään tukiasemalle. Ylävirran tietoliikenne ei siis tarvitse erillisiä kanavanvarausmenettelyjä, ja yhteys on jatkuvasti käytettävissä release 99:n mukaisen verkon tavoin. HSUPA käyttää datan siirtoon E-DCH-kuljetuskanavaa (Enhanched Data Channel). E-DCH-kanavan data puolestaan siirretään fyysisellä E-DPDCH-kanavalla (Enhanched Dedicated Physical Data Channel). Taulukossa 3 nähdään HSUPA:n 6 kategoriaa ja niitä vastaavat suoritusarvot. Taulukon siirtonopeudet ovat teoreettisia maksiminopeuksia. (Granlund 2007, 433.)

TAULUKKO 3. HSUPA suorituskykyluokat (Granlund 2007, 436)

E-DCH luokka	E-DCH hajautus-koodien lkm	TTI ms	Bitit/jakso TTI = 10	Bitit/jakso TTI = 2	Siirto-nopeus Mbit/s
Category 1	1	10	7296	-	0,76
Category 2	2	10 ja 2	14592	2919	1,46
Category 3	2	10	14592	-	1,46
Category 4	2	10 ja 2	20000	5837	2,92
Category 5	2	10	20000	-	2,00
Category 6	4	10 ja 2	20000	11520	5,76

2.2.3 Evolved HSPA ja DC-HSPA

Evolved HSPA on HSPA:n paranneltu versio, joka otettiin käyttöön 3GPP:n release 7:ssä. Evolved HSPA, toiselta nimeltään HSPA+, parantaa HSPA:n käsittämien HSDPA:n ja HSUPA:n siirtonopeuksia. HSPA+:ssa on monia uusia ominaisuuksia ja parannuksia perus-HSPA-tekniikkaan nähden. Yksi olennaisimmista muutoksista on MIMO-tekniikan (Multiple Input Multiple Output) käyttöönotto. Käytännössä MIMO tarkoittaa useamman lähetys- ja vastaanottoantennin käyttöä. Jos MIMO:n tarvitsemia useita antenneja ei ole käytettävissä, voidaan HSPA+:lla käyttää 64-QAM-modulaatiota signaalitason ollessa tarpeeksi korkea. (Evolved HSPA / HSPA+ 2011.)

DC-HSPA (Dual Carrier High Speed Packet Access) on HSPA:n kehittynyt versio, joka käyttää kahta kantoaaltoa. 3GPP:n release 8:ssa otettiin käyttöön DC-HSDPA (Dual Carrier High Speed Downlink Packet Access), joka on siis kahta kantoaaltoa käyttävä kehittynyt HSDPA-tekniikka. DC-HSDPA:lla päästään entistä suurempiin siirtonopeuksiin. Release 9:ssä voidaan lisäksi käyttää MIMO-tekniikkaa DC-HSDPA:n kanssa. Release 9:ssä otettiin myös käyttöön DC-HSUPA (Dual Carrier High Speed Uplink Packet Access), jolla puolestaan nostetaan ylävirran siirtonopeuksia. (Dual Carrier HSPA 2011.)

2.3 LTE ja tulevaisuus

Kolmannen sukupolven tekniikoiden kehittyessä tulee vastaan raja, jonka jälkeen vaatimukset täyttävät tekniikat voidaan luokitella neljänteen sukupolveen eli 4G-tekniikoiksi (Fourth Generation). ITU:n radioviestintäsektori ITU-R (International Telecommunication Union Radiocommunication Sector) on määritellyt 4G:n IMT-Advanced -vaatimukset. Olennaisin 4G:n vaatimus on sen siirtonopeus, joka määritellään 100 Mbit/s korkean liikkuvuuden tietoliikenteelle ja 1 Gbit/s vähäisen liikkuvuuden tietoliikenteelle. Vähäiseen liikkuvuuteen lasketaan mm. kävelijät ja paikallaan olevat käyttäjät, kun taas korkea liikkuvuus kattaa esimerkiksi junat ja autot. (IMT-advanced 2010.)

LTE (Long Term Evolution) on HSPA:n tavoin UMTS-järjestelmästä kehitetty saman ns. teknologiapuun 4G-tekniikka, vaikka LTE:n kutsumisesta 4G-tekniikaksi on kiistelty. ITU hyväksyi LTE-tekniikan täyttävän 4G:n IMT-Advanced -vaatimukset vasta joulukuussa 2010, vaikka LTE on ollut markkinoilla jo vuodesta 2009. LTE eroaa edeltäjistään huomattavasti, sillä aikaisemmissa järjestelmissä käytettävä WCDMA-tekniikka on muuttunut OFDMA- (Orthogonal Frequency Division Multiple Access) ja SC-FDMA-tekniikoiden (Single Carrier Frequency Division Multiple Access) yhdistelmäksi. LTE käyttää siis ylä- ja alavirrassa eri tekniikoita. OFDMA-tekniikkaa käytetään alavirrassa, kun taas SC-FDMA-tekniikkaa on käytössä ylävirrassa. OFDMA-tekniikan etuna on korkea sietokyky heijastuksille ja häiriöille, vaikka sillä on myös korkea siirtonopeus. Ylävirrassa käytettävän SC-FDMA:n etu on puolestaan vähäisempi tehon käyttö,

mikä on tärkeää akkuvirtaa käyttävälle laitteelle. LTE:ssä on monia yhtäläisyyksiä sen edeltäjiin, joten osittainen tekniikoiden uudelleenkäyttö on mahdollista. Monet LTE:n tuomat parannukset ovat myös samanlaisia kuin edeltävissä tekniikoissa. Pääasiassa LTE kasvattaa siirtonopeuksia, parantaa palveluita, vähentää kuluja ja lyhentää viiveitä. LTE:ssä voidaan käyttää MIMO-tekniikkaa eli useampia lähetys- ja vastaanottoantenneja, joita voi olla joko 2 tai 4. LTE tarjoaa siis 100 – 326 Mbit/s siirtonopeuden alavirtaan ja 50 – 86 Mbit/s siirtonopeuden ylävirtaan, riippuen käytettävien antennien lukumäärästä. (3G LTE Tutorial 2011.)

LTE:stä on myös kehitetty vasta testivaiheessa oleva LTE Advanced, jonka tarkoituksena on tarjota yhä parempi 4G:n vaatimusten mukainen siirtonopeus, ja tehdä LTE-tekniikasta virallisesti neljännen sukupolven tekniikka. LTE Advanced:n tavoitteena on siis saada 1 Gbit/s siirtonopeus alavirtaan ja 500 Mbit/s ylävirtaan. Taulukossa 4 vertaillaan UMTS-teknologiapuun tekniikoita. Taulukon maksimisiirtonopeudet ovat teoreettisia eikä niissä oteta huomioon esimerkiksi MIMO:n käyttöä, jolla HSPA+:n ja LTE:n siirtonopeudet saataisiin korkeammiksi. (4G LTE Advanced Tutorial 2011.)

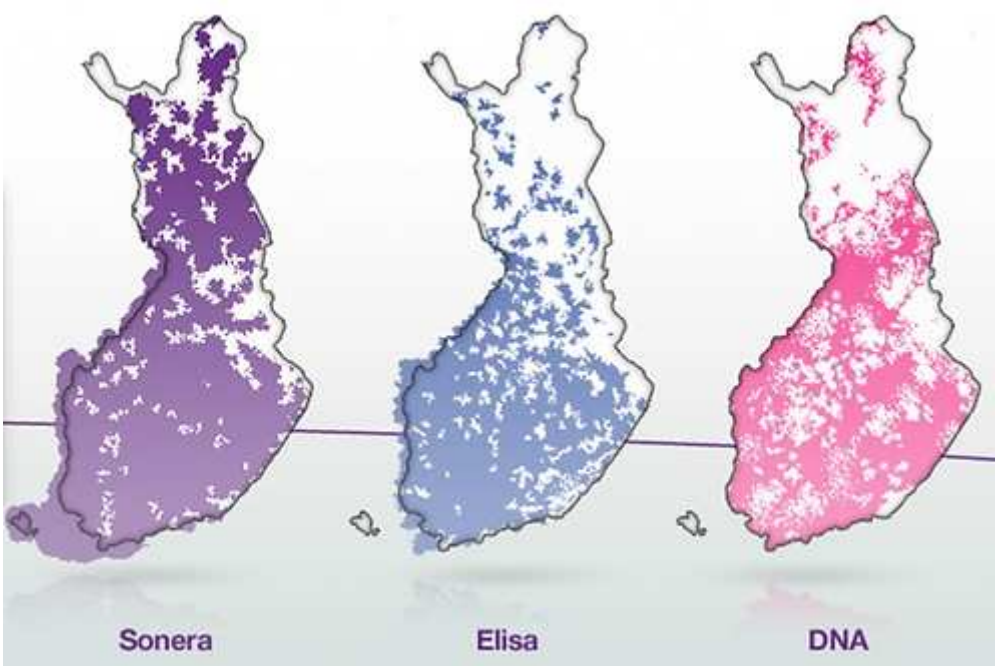
TAULUKKO 4. Tekniikoiden vertailu (4G LTE Advanced Tutorial 2011)

	WCDMA (UMTS)	HSPA HSDPA / HSUPA	HSPA+	LTE	LTE ADVANCED (IMT ADVANCED)
Max downlink speed bps	384 k	14 M	28 M	100M	1G
Max uplink speed bps	128 k	5.7 M	11 M	50 M	500 M
Latency round trip time approx	150 ms	100 ms	50ms (max)	~10 ms	less than 5 ms
3GPP releases	Rel 99/4	Rel 5 / 6	Rel 7	Rel 8	Rel 10
Approx years of initial roll out	2003 / 4	2005 / 6 HSDPA 2007 / 8 HSUPA	2008 / 9	2009 / 10	
Access methodology	CDMA	CDMA	CDMA	OFDMA / SC-FDMA	OFDMA / SC-FDMA

2.4 UMTS-verkot Suomessa

Suomen UMTS-verkkoja ylläpitää Viestintävirastolta toimiluvat saaneet teleoperaattorit, jotka ovat TeliaSonera, Elisa ja DNA. Lisäksi Ålands Mobiltelefon AB ylläpitää Ahvenanmaan 3G-verkkoa. Muillakin operaattoreilla on UMTS-mobiililaajakaistapalveluita, mutta ne käyttävät toimilupien saamien operaattorien radioverkkoja. Suomen UMTS-verkoissa käytetään joko UMTS 2100- tai UMTS 900 -taajuuskaistoja, joista UMTS 2100:n kuuluvuusalueet ovat pääosin kaupunkien alueilla. UMTS 900:n paremman kuuluvuusalueen ansiosta sitä käytetään kaupunkialueiden ulkopuolella, maaseuduilla ja muilla vähemmän asutuilla alueilla. (Operaattoreiden kuuluvuuskartat 2011.)

Suomen UMTS-verkkojen kuuluvuusalueet ja siirtonopeudet vaihtelevat suuresti tukiaseman sijainnin ja käytetyn UMTS-tekniikan mukaan. Kuviossa 4 nähdään TeliaSoneran, Elisan ja DNA:n UMTS-kuuluvuusalueet, joilla käytetään UMTS 2100- ja UMTS 900 -taajuuskaistoja. Kyseisillä kuuluvuusalueilla on minimissään käytössä UMTS-tekniikka ilman HSPA:ta, joten siirtonopeuden on oltava vähintään teoreettinen maksimi 384 kbit/s. HSPA-tekniikka on suurimmaksi osin käytössä vasta kaupunkiseuduilla, josta se leviää tukiasemien uudistuessa vähemmän asutuille alueille. Tukiaseman tekniikan lisäksi operaattorit voivat asettaa rajoituksia omiin liittymiinsä. TeliaSonera ilmoittaa 3G-verkkonsa nopeimmiksi käytettäviksi tekniikoiksi HSDPA:n ja HSUPA:n, joiden teoreettisiksi maksiminopeuksiksi annetaan 7,2 Mbit/s alavirtaan ja 2,0 Mbit/s ylävirtaan. Huomataan kuitenkin, että tekniikoiden spesifikaatioiden teoreettiset maksiminopeudet ovat huomattavasti suuremmat. TeliaSonera on myös ottanut käyttöön Helsingissä ja Turussa 4G LTE-tekniikan, jolle ilmoitetaan teoreettiseksi maksiminopeudeksi 100 Mbit/s. (3G ja 4G 2011.)



KUVIO 4. Suomen operaattorien UMTS-kuuluvuusalueet 7.7.2011 (3G-kuuluvuusalueet 2011)

DNA käyttää pääkaupunkiseudulla uutta DC-HSPA+-tekniikkaa, jolle ilmoitetaan teoreettiseksi maksiminopeudeksi 42 Mbit/s. DNA käyttää laajemmin HSPA+-tekniikkaa, jolle se ilmoittaa teoreettiseksi maksiminopeudeksi 21 Mbit/s. (DNA Mokkula MC545 2011). DNA:lla on myös testivaiheessa 4G-verkko, jonka kuuluvuusalueet rajoittuvat Helsingin ja Hämeenlinnan keskustoihin (DNA 4G 2011). Elisan tytäryhtiö ja sen 3G-verkkoa käyttävä Saunalahti ilmoittaa nopeimman liittymänsä alavirran maksiminopeudeksi myös 42 Mbit/s, joka vastaa DNA:n tavoin DC-HSPA+-tekniikan teoreettista maksiminopeutta. Ylävirran teoreettiseksi maksiminopeudeksi ilmoitetaan 5,76 Mbit/s, joka vastaa HSUPA:n kategorian 6 siirtonopeutta. (Nettitikku E398 2011.)

3 UMTS-ANTENNIT

3.1 Antennityypit

Lähes kaikissa 3G-laitteissa, kuten 3G-modeemeissa ja 3G-reitittimissä on käytännössä jonkinlainen oma antenni. Useimmiten antenni on joko 3G-modeemeissa sisäinen tai 3G-reitittimissä pieni laitteeseen kierrettävä ulkoinen antenni. Laitteiden omien antennien etuna on yleisesti niiden kestävyys ja pieni koko. Antennien huonona puolena on niiden heikko kuuluvuus varsinkin 3G-modeemien sisäisillä antenneilla. Kyseiset antennit ovat usein ympärisäteileviä, jolloin niillä on erityisen heikko kuuluvuus esimerkiksi tukiaseman kantaman reuna-alueilla. Laitteiden omien antennien käyttö ei ole kuitenkaan välttämätöntä. Kuuluvuutta voidaan lisätä erityyppisillä lisäantenneilla, jotka voidaan luokitella usealla tavalla. (Antennin valinta 2011.)

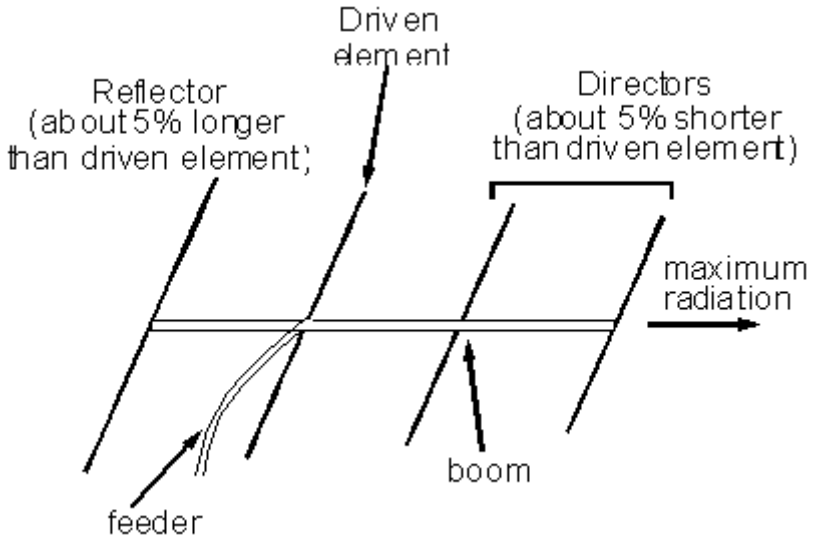
Yleisimmin puhutaan joko ympärisäteilevistä tai suunta-antenneista. Suunta-antennit soveltuvat parhaiten asennuksiin, jotka ovat kiinteitä ja kaukana tukiasemasta. Suunta-antennit eivät sovi puolestaan liikkuvaan käyttöön, sillä suunta-antenni on suunnattava tukiasemaan mahdollisimman tarkasti, jos halutaan optimaalinen yhteys. Liikkuvassa käytössä tukiaseman suunta vaihtuu jatkuvasti, jolloin ympärisäteilevän antennin käyttö on suositeltavaa. Antennit voidaan myös jakaa sisä- ja ulkoantenneihin sekä yksitaajuus- ja laajakaista-antenneihin. Sisäantennit ovat pääasiassa ympärisäteileviä, kun taas ulkoantennit voivat olla joko suunta-antenneja tai ympärisäteileviä. Yksitaajuusantennit käyttävät tiettyä taajuusaluetta, ja laajakaista-antennit voivat käyttää useita UMTS-taajuuskaistoja kuten 900, 1800 ja 2100. (Antennin valinta 2011.)

3.1.1 Jagiantenni

Yksi suosituimmista suunta-antenneista on jagiantenni, jota kutsutaan myös nimillä Yagi-antenni tai Yagi-uda-antenni. Jagiantennia käytetään monenlaisissa asennuksissa, joissa tarvitaan suurta antennivahvistusta ja suuntaavuutta. Jagiantenni on erityisen suosittu televisiovastaanotossa. Jagiantenni koostuu useasta elemen-

tistä, jotka ovat heijastaja, säteilijä ja ohjaajat. Säteilevä elementti on dipoli, joka on ainoa sähköisesti kytketty elementti. Muut elementit ovat ns. loiselementtejä, jotka uudelleensäteilevät dipolilta vastaanotetun tehon. Loiselementit uudelleensäteilevät signaalinsa hieman eri vaiheessa kuin säteilijä, mikä vahvistaa signaalia tiettyihin suuntiin ja kumoaa toisiin suuntiin. (Yagi 2011.)

Loiselementit ovat joko kapasitiivisia tai induktiivisia. Kapasitiivisuus ja induktiivisuus saavutetaan tekemällä loiselementistä säteilijää pidempi tai lyhyempi. Heijastajan tulee olla induktiivinen, jolloin siihen tuleva säteily heijastuu. Heijastajan induktiivisuus siis saavutetaan tekemällä siitä 5 % pidempi kuin säteilijä. Ohjaajien puolestaan tulee olla kapasitiivisia, jolloin ne ohjaavat tulevan säteilyn elementtien suuntaan. Ohjaajien kapasitiivisuus saavutetaan tekemällä niistä 5 % lyhyemmät kuin säteilijä. (Yagi 2011.)

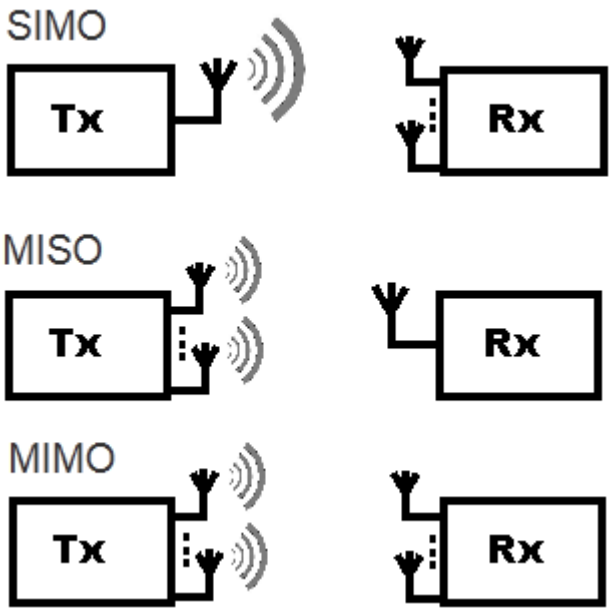


KUVIO 5. Jagiantennin rakenne (Yagi 2011)

3.1.2 Usean antennin järjestelmät

Siirtonopeuden tai kuuluvuusalueen kattavuuden lisäämiseksi voidaan käyttää useampaa lähetys- ja vastaanottoantennia, jos laitteet mahdollistavat sen. Usean antennin järjestelmät voidaan jakaa kolmeen eri luokkaan, joita ovat MISO (Multiple Input Single Output), SIMO (Single Input Multiple Output) ja edellä mainittu

MIMO. MISO-järjestelmässä käytetään useaa lähetysantennia, jolloin signaalin kestävyys kasvaa. MISO ei siis nosta siirtonopeutta, vaan kasvattaa kuuluvuusalueen kattavuutta. MISO on myös nimeltään Tx diversity. SIMO-järjestelmässä puolestaan käytetään useaa vastaanottoantennia, mikä nostaa SNR:ta (Signal-to-Noise Ratio) yhdistämällä usean kopion samasta signaalista. SIMO ei myöskään nosta siirtonopeutta, vaan kasvattaa kuuluvuusalueen kattavuutta. SIMO:sta käytetään nimitystä Rx diversity. Kuviossa 6 on esitetty usean antennin järjestelmien rakenteet. (LTE MIMO System-Level Design 2009.)



KUVIO 6. Usean antennin järjestelmien rakenteet (MIMO Formats 2011)

Usealla antennilla voidaan signaalin kestävyyden lisäksi kasvattaa siirtonopeutta, jos käytetään MIMO-järjestelmää, jossa radiolinkin molemmissa päissä on useita antenneja. MIMO:ssa siirtonopeuden kasvun mahdollistaa signaalin kanavointi. Lähetysvirta siis jaetaan useaan osaan, jolloin jokainen antenni lähettää jaetun osan tietyllä radiotien polulla, jotka mahdollistetaan antennien eri sijainneilla. MIMO:ssa jokainen vastaanottoantenni käyttää eri signaalia, kun taas SIMO-järjestelmässä vastaanottavat antennit käyttävät saman signaalin kopioita. Kanavoitu lähetysvirta yhdistetään lopulta, kun lähetysvirta on vastaanotettu. Tämä mahdollistaa siirtonopeuden kasvun käyttämättä suurempaa kaistanleveyttä, mikä tekee MIMO-järjestelmästä tärkeän osan uusimmille tekniikoille kuten HSPA+ ja LTE. (MIMO Technology Tutorial 2011.)

3.2 Antennin käyttöönotto

Käyttäjän ottaessa 3G-laitetta käyttöön on ennen lisäantennin hankintaa tutkittava alueen 3G-kuuluvuutta, joka saadaan selville oman operaattorin kuuluvuusaluekartasta. Kuuluvuusaluekartan tutkiminen ei kuitenkaan riitä, vaan on myös otettava huomioon mahdolliset esteet tukiaseman ja käytettävän antennin välillä. Olennaisimpia esteitä ovat korkeat maaston kohoumat, puusto ja rakennukset. Mahdolliset esteet voidaan minimoida asentamalla antenni mahdollisimman korkealle, esimerkiksi katolle. On myös otettava huomioon antennin ja laitteen välisen kaapelin pituus, sillä kaapeli vaimentaa signaalia n. 0,5 dBi/m kaapelin tyypistä riippuen. (Kuinka suunta-antenni suunnataan kotikonstein? 2011.)

Lisäantennia voidaan käyttää, jos alueen UMTS-kuuluvuus on heikko tai halutaan parantaa siirtonopeutta. Tällöin on otettava selvää tukiaseman sijainnista, jos käytetään suunta-antennia. Käytettäessä ympärisäteilevää lisäantennia ei tukiaseman sijainnilla ole niinkään väliä, ja antenni voidaan asentaa yksinkertaisesti mahdollisimman korkealle. Tukiasemien sijainteja ei kuitenkaan merkitä kuuluvuusaluekarttoihin, joten sijainti on selvitettävä antennin avulla, jos tukiaseman sijainti ei ole ennalta tiedossa. Suunta-antennilla voidaan etsiä tukiaseman karkea sijainti suuntaamalla antenni eri suuntiin, joissa testataan yksittäin 3G-yhteyden laatu. Vaihtoehtoisesti tukiasemien paikantamiseen voidaan myös käyttää erilaisia tukiasematietokantoja, kuten OpenSignalMaps (http://opensignalmaps.com/), jossa näkyy varsinkin monet Elisan tukiasemat. Kun tiedossa on karkea tukiaseman suunta tai sijainti, voidaan se tarkistaa Kansalaisen Karttapaikka -palvelusta (http://*kansalaisen.karttapaikka.fi/*), jossa tukiasemat ovat merkitty karttaan symboleilla. Lopulta voidaan hienosäätää antennin suunta kääntämällä sitä muutamia millimetrejä kerrallaan, jotta saataisiin optimaalinen yhteys tukiasemaan. Yhteys voidaan testata käyttämällä eri nopeustestipalveluja tai mahdollisesti laitteen omaa ohjelmistoa. (Kuinka suunta-antenni suunnataan kotikonstein? 2011.)

Antennin käytössä ja suuntamittauksissa olennaisin termi on RSSI (Received Signal Strength Indicator), joka on kokonaisen vastaanotetun signaalin teho. RSSI ei kuitenkaan kerro mahdollisista häiriötekijöistä, joiden vaikutus varsinaiseen UMTS-verkon fyysisen kanavan tehoon voidaan mitata termillä EC/IO. EC/IO

kuvaa fyysisen kanavan tehon suhdetta kokonaiseen vastaanotetun signaalin tehoon. Lopullinen EC/IO-arvo mitataan dBm:nä RSSI:n tavoin. EC/IO-arvo voi korkeintaan olla 0 dBm, jolloin signaalin laatu on paras mahdollinen. Yhteys toimii vielä -10 dBm:n EC/IO-arvolla, mutta alhaisemmilla EC/IO-arvoilla syntyy pakettien häviötä ja latenssi kasvaa huomattavasti. (What is Ec/Io 2011.)

4 3G-REITITTIMEN TIETOTURVA

4.1 Pakettisuodattava palomuuri

3G-reitittimiin sisältyy useimmiten jonkinlainen palomuuri. Yleisin ja yksinkertaisin 3G-reitittimiin sisältyvä palomuuritekniikka on pakettisuodatus, jossa palomuuri tarkistaa IP-pakettien (Internet Protocol) porttinumeron sekä lähtö- ja kohdeosoitteet. Käyttäjän tehtävänä on määritellä pakettisuodattavaan palomuuriin säännöt, jotka puolestaan määrittelevät, mitkä osoitteet ja portit ovat sallittuja eri tilanteissa. Palomuurin tarkistetut paketit joko hylätään tai hyväksytään. TCP/IP-protokolla (Transmission Control Protocol / Internet Protocol) on kuitenkin teknisesti monimutkainen, joten sillä on mahdollista suorittaa monenlaisia hyökkäyksiä. Nämä yksinkertaisimmat pakettisuodattavat palomuurit ovat toiselta nimeltään tilattomia palomuureja. (Järvinen 2002, 316 - 317.)

Kehittyneemmät palomuurit osaavat tarkkailla myös pakettien sisältöä ja niiden järjestystä. Tällöin palomuuri tutkii aktiivilaitteen TCP-yhteyden tilan ja hyväksyy vain paketit, jotka ovat loogisesti oikeita. Liikennöinnin tilaa tutkimalla voidaan torjua palvelunestohyökkäyksiä ja IP-osoitteiden väärennösyrityksiä, joilla saadaan hyökkäävä laite kuulumaan sisäverkkoon. Liikennöinnin tilan tutkiminen antaa myös hälytyksen porttiskannauksesta. Tällaisia kehittyneempiä palomuureja kutsutaan tilallisiksi eli dynaamisiksi pakettisuotimiksi. Pakettisuodattavat palomuurit toimivat kuljetuskerroksella. (Järvinen 2002, 316 - 317.)

4.2 VPN

Etähallinnassa, yksi turvallisimmista tietoturvamenetelmistä on VPN. Monista 3G-reitittimistä löytyy VPN-tuki, joka on hyödyllinen ominaisuus varsinkin etähallinnassa. VPN-tuen avulla voidaan yhdistää lähiverkkoja Internetin yli yhdeksi kokonaisuudeksi, jos lähiverkoilla on VPN-yhteyttä tukeva laite Internet-yhteyden rajapinnassa. VPN:ää voidaan käyttää myös yksittäisen tietokoneen ja VPN-laitteen yhteydessä olevan lähiverkon välillä, jos tietokoneessa on VPN-mahdollisuus. Esimerkiksi yritysverkoissa työntekijät voivat käyttää toisessa toi-

mipisteessä olevan lähiverkon resursseja aivan kuin kyseessä olisi yksi lähiverkko. Internetin yli muodostettu VPN-yhteys on tietoturvallinen, sillä muodostetussa VPN-tunnelissa kulkeva tieto on salattu. (Järvinen 2002, 318 – 319.)

Yksityinen verkko muodostetaan Internetin yli tunneloimalla, jossa lähetettävä datapaketti kapseloidaan toisen paketin sisälle. Vastaanottavan laitteen on puolestaan tunnistettava ulkoisen paketin protokolla, jotta paketti voidaan vastaanottaa. Tunnelointi koostuu kolmesta eri protokollasta, jotka ovat kuljettava protokolla, kapselointiprotokolla ja siirtoprotokolla. Kuljetettavalla protokollalla tarkoitetaan alkuperäistä datapakettia, joka on usein IP-paketti tai jokin vastaava OSI-mallin (Open Systems Interconnection) verkkokerroksen protokolla. Alkuperäinen datapaketti kapseloidaan jollakin kapselointiprotokollalla, joita ovat esimerkiksi GRE (Generic Routing Encapsulation), IPSec (Internet Protocol Security) ja PPTP (Point-to-Point Tunneling Protocol). Työssä käsitellään tarkemmin IPSec- ja PPTP-kapselointiprotokollia. Käytetyn protokollan on oltava tuettuna tunnelin kummassakin päässä, jotta tunneli toimisi oikein. Kapseloitu paketti asetetaan vielä siirtoprotkollan otsikon sisään, jotta data voidaan lähettää julkisessa verkossa. Yleisin siirtoprotkolla on IP. Kapselointi siis mahdollistaa, että VPN-tunneloinnilla voidaan käyttää protokollia, joita ei normaalisti tueta Internetissä. (Thomas 2005, 247.)

Tunnelointi ei kuitenkaan riitä yksityisyyden takaamiseksi, vaan VPN-liikenne on myös salattava. Salauksessa käytetään kapselointiprotokollia, kuten IPSec tai GRE, joita käytetään yleensä toimipisteiden välisissä VPN-verkoissa. IPSec ja GRE eroavat toisistaan tietoturvassa ja toiminnallisuudessa. IPSec tarjoaa paremman tietoturvan, mutta pystyy tunneloimaan ja salaamaan vain IP-paketteja. GRE puolestaan voi tunneloida ja salata IP-pakettien lisäksi muitakin paketteja. (Thomas 2005, 248.)

4.2.1 IPSec

VPN-ratkaisuista IPSec on teollisuusstandardin mukainen protokolla, joka suojaa ja todentaa IP-paketit IPSec-laitteiden välillä. IPSec toimii OSI-mallin verkkokerroksella ja tarjoaa verkon tietoturvapalveluita, joita ovat datan luotettavuus, datan eheys, datan alkuperän todennus ja uudelleensoiton esto. Lähetettävät paketit salataan ennen kuin paketit lähetetään verkkoon, jolloin mahdollinen ulkopuolinen henkilö ei pysty lukemaan dataa. Vastaanottavassa päässä puolestaan todennetaan vastaanotetut paketit, jotta varmistutaan, että dataa ei ole muutettu tiedonsiirron aikana. Vastaanottava pää voi myös todentaa vastaanotettujen pakettien lähteen sekä havaita, että hylätä uudelleensoitetut paketit. (Thomas 2005, 243 – 244.)

IPSec:llä on tunneli- ja siirtotilalle eri salausmuodot, jotka eroavat toisistaan kuljetettavan paketin lisäkuorman ja sovelluskohteen mukaan. Tunnelimuodossa IPSec toimii kahden tietoturvayhdyskäytävän välillä. Tunnelimuodossa suojataan ja kapseloidaan kokonainen IP-paketti eli paketin otsikko ja hyötykuorma, kun taas siirtomuodossa salataan vain hyötykuorma. Tunnelimuoto on siis paljon turvallisempi kuin siirtomuoto. (Thomas 2005, 248 – 249.)

IPSec muodostaa yhtenäisen ja turvallisen, standardien mukaisen kehyksen, käyttämällä kolmea toisiaan täydentävää protokollaa. IPSec-yhteyden neuvotteluvaiheen kuvaa ISAKMP (Internet Security Association Key Managemenet Protocol), joka määritellään todennetun avaintenvaihdon suorittamiseksi. Avaimet voidaan luoda esimerkiksi Diffie-Hellmanin algoritmilla. Kehyksen turvaparametrien neuvottelemiselle tarjoaa ISAKMP:n sisältämä IKE (Internet Key Exchange), joka on turvallisen kommunikaatiokanavan tarjoava kaksisuuntainen protokolla. Turvaparametrejä ovat salausalgoritmi, tiivistysalgoritmi, todennus ja turva-assosiaation elinikä sekunneissa. Muita IPSec-standardin protokollia ovat ESP (Encapsulated Security Protocol) ja AH (Authentication header), jotka tarjoavat mm. todennuksen tunnelimuodossa. Kuviossa 7 on esitetty IPSec-yhteyden neuvotteluvaiheet. Neuvottelun ensimmäiselle vaiheelle eli IKE-vaiheelle 1 voidaan määritellä 2 eri tilaa, jotka ovat aggressiivinen ja main-tila. Main-tilassa todennuksella on kaikki 4 vaihetta, kun taas aggressiivisessa tilassa ohitetaan useita IKE-todennuksen vaiheita, jolloin todennus jää vain kolmivaiheiseksi. Aggressiivinen tila on siis nope-

ampi, mutta sitä pidetään vähemmän turvallisena kuin main-tilaa. (Thomas 2005, 250 – 260.)

KUVIO 7. VPN-yhteydenmuodostus IPSec:llä (Thomas 2005, 259)

4.2.2 PPTP

IPSec-protokollan ollessa yksi yleisimmin käytetyistä ja turvallisimmista VPN-protokollista VPN-etäyhteyksissä käytetään myös paljon PPTP-pohjaisia ratkaisuja. PPTP:n on kehittänyt Ascend Communications, 3Com/Primary Access, ECI Telematics, U.S. Robotics ja Microsoft Corporation. Microsoft on ollut yhtenä päätekijänä PPTP:n suosiossa, sillä Windows-käyttöjärjestelmien mukana tulevat VPN-ominaisuudet perustuvat pääosin PPTP:seen. PPTP:n suosiosta huolimatta sillä on joitakin haittapuolia. PPTP ei esimerkiksi määrittele, miten todennus ja datan salaus tulisi toteuttaa. Tämä voi aiheuttaa yhteensopivuusongelmia eri valmistajien välisissä VPN-laitteissa, jos laitteet esimerkiksi käyttävät eri autentikointiprotokollia. PPTP-yhteyden turvallisuus on myös huomattavasti heikompi muihin VPN-ratkaisuihin verrattuna. (Thomas 2005, 135 – 138.)

IPSec:stä eroavasti PPTP toimii OSI-mallin siirtokerroksella. PPTP perustuu PPP-protokollastandardiin (Point-to-Point Protocol), joka on kehitetty soittoyhteyksiä varten. PPTP:n toiminta perustuu datan paketoimiseen PPP-paketteihin, jotka puolestaan kapsuloidaan VPN-tunneliin lähetettäviin IP-paketteihin. PPTP tukee pakettien pakkausta ja datan salausta, ja PPTP hyödyntää GRE-protokollaa pakettien tunneloimiseen ja välittämiseen. (Thomas 2005, 135 – 137.)

PPTP:n todennuksessa käytetään erilaisia autentikointiprotokollia, kuten CHAP (Challenge-Handshake Authentication Protocol), PAP (Password Authentication Protocol) tai MS_CHAPv2 (Microsoft Challenge-Handshake Protocol version 2). CHAP on kolmivaiheinen kättely-yhteyskäytäntö, jossa käytettävää salasanaa ei lähetetä linkin yli. Linkin muodostuttua palvelin lähettää haasteviestin yhteyden muodostajalle eli asiakkaalle. Asiakas muodostaa tiivistefunktiolla haasteviestistä ja salasanasta vastauksen, joka lähetetään palvelimelle. Palvelin vertaa vastausta omaan tiivistefunktiolla muodostettuun arvoon. Jos vastaus ja palvelin oma arvo täsmäävät, todennus hyväksytään ja palvelin lähettää kuittauksen onnistumisesta asiakkaalle. Jos arvot eivät täsmää, yhteys yleisesti katkaistaan ja palvelin lähettää viestin epäonnistumisesta. PAP on puolestaan kaksivaiheinen kättely-yhteyskäytäntö, jossa käyttäjänimi ja salasana lähetetään salaamattomana linkin yli. PAP:ssa asiakas lähettää käyttäjänimen ja salasanan salaamattomana palvelimelle, joka vertaa käyttäjätietoja palvelimeen määriteltyihin tietoihin. Palvelin vastaa viestiin kuittauksella, jolla hyväksytään tai hylätään yhteys. CHAP on huomattavasti turvallisempi protokolla kuin PAP. (Identify authentication protocols 2010; CHAP 2000.)

MS_CHAPv2 on Microsoftin kehittämä versio CHAP:sta. MS_CHAPv2 toimii samalla kolmivaiheperiaatteella kuin CHAP, mutta MS_CHAPv2 tarjoaa kaksisuuntaisen autentikoinnin palvelimen ja asiakkaan välillä. Asiakkaan vastausviestissä on mukana asiakkaan oma haasteviesti, johon palvelin vastaa lopullisen kuittauksen yhteydessä omalla vastauksellaan. Asiakas ei kuittaa palvelimen autentikointivastausta, vaan muodostaa yhteyden ainoastaan, jos autentikointivastaus on oikea. MS_CHAPv2 tukee myös auntentikoinnin ja salasanan uusintamekanismeja. (RFC 2759 2000.)

5 TUTKITTAVAT 3G-REITITTIMET

5.1 3G-reitittimet ja niiden ominaisuudet

Työssä tutkittavat ja vertailtavat 3G-reitittimet ovat Sierra Airlink Raven XE (Raven XE) ja TeleWell 3G Flash-OFDM-reititin (TeleWell 3G-reititin). 3G-reitittimiä voidaan kutsua myös 3G-yhdyskäytäviksi. Tutkittavien laitteiden tekniikoissa ja ominaisuuksissa ei ole kuitenkaan monia yhtäläisyyksiä, vaikka molemmilla laitteilla voidaan toteuttaa laitteiden etähallinta 3G-verkossa. Mahdollisesta saman tyyppisestä käytöstä huolimatta laitteet on suunniteltu eri käyttötarkoituksiin. Raven XE on tarkoitettu yritys- ja teollisuuskäyttöön, kun taas TeleWell 3G -reititin sopii paremmin kuluttajille ja pienyrityksille. Käyttötarkoitukset jakavat myös laitteet eri hintaluokkiin, jotka ovat 50-100 € TeleWell 3G -reitittimelle ja n. 400 € Raven XE:lle.

Laitteiden olennaisin ero on niiden käyttämä 3G-tekniikka. Raven XE voi käyttää joko UMTS:ään perustuvaa HSDPA- ja HSUPA-tekniikkaa tai Euroopassa vähemmän suosittuun CDMA2000:een perustuvaa EV-DO Rev. A -tekniikkaa (Evolution-Data Optimized). Tukiasemassa käytettävän tekniikkatason mukaan Raven XE voi myös käyttää joko UMTS- tai CDMA2000-tekniikkapuiden edeltäviä tekniikoita. TeleWell 3G -reitittimessä puolestaan ei ole sisäistä 3G-tekniikkaa, joten siinä on käytettävä joko PC Card- tai USB (Universal Serial Bus) 3G-modeemikorttia. TeleWell 3G -reitittimen 3G-tekniikan siis määrää siinä käytettävä 3G-modeemikortti. Tämä tuo laitteelle päivitettävyyttä, mutta on myös otettava huomioon mahdolliset yhteensopivuusongelmat laajan 3G-modeemikorttivalikoiman vuoksi. TeleWell 3G -reitittimellä voidaan myös käyttää vaihtoehtoisesti Flash-OFDM-tekniikkaan (Fast Low-latency Access with Seamless Handoff - Orthogonal Frequency Division Multiplexing) perustuvaa @450-verkkoa, jos käytettävä PC Card- tai USB-modeemikortti mahdollistaa sen.

Laitteiden eri käyttötarkoitukset ja tekniikat huomataan myös liitännöistä. Raven XE:ssä on SMA-naaras-liitännät (SubMiniature version A) kahdelle ulkoiselle 3G-antennille, 2 ohjelmoitavaa I/O-porttia (Input / Output), ethernet-liitin ja vaih-

toehtoinen USB mini-B -liitin etähallittavalle laitteelle. Kuviosta 8 nähdään Raven XE:n liitännät. Yksittäinen ethernet-portti kertoo sen, että laite on pääasiassa tarkoitettu yksittäisten laitteiden etähallintaan, vaikka muodostettava 3G-yhteys voidaan myös jakaa usealle laitteelle esimerkiksi erillisellä kytkimellä. Kahdesta ulkoisesta antenniliitännästä voidaan päätellä, että laitteen käyttötarkoitukseen halutaan mahdollisimman luotettava 3G-yhteys, kuten teollisuuskäytössä tai muussa yrityskäytössä vaaditaan. Raven XE on myös lujatekoinen ja suunniteltu kestämään tärinää, pölyä, kosteutta ja äärimmäisiä lämpötiloja.

KUVIO 8. Sierra Airlink Raven XE

TeleWell 3G -reititin on sen sijaan pääasiassa tarkoitettu 3G- tai @450-yhteyden jakamiseen usealle laitteelle. Yhteyden jakaminen on toteutettu ethernet-portin lisäksi langattomasti WLAN-tekniikalla (Wireless Local Area Network). 3G- ja @450-yhteysmahdollisuuksien lisäksi Internet-yhteys voidaan myös luoda kiinteällä laajakaistalla käyttämällä laitteen WAN-ethernet-porttia (Wide Area Network). Ensisijainen kiinteä yhteys voidaan tällöin varmistaa langattomalla yhtey-

dellä. Laitteessa on siis liitännät PC Card- ja USB-modeemikorteille, ethernet-liitännät ulko- ja sisäverkolle sekä antenniliitin WLAN-antennille. Huomataan, että mahdollinen 3G-lisäantenni on kiinnitettävä suoraan 3G-modeemikorttiin, jos kortissa on liitin lisäantennille. Kuviosta 9 nähdään TeleWell 3G -reitittimen liitännät.

KUVIO 9. TeleWell 3G Flash-OFDM-reititin

Sovellustasolla Raven XE:llä on enemmän ominaisuuksia kuin TeleWell 3G -reitittimellä. Monet TeleWell 3G -reitittimestä poikkeavat ominaisuudet liittyvät etähallintaan, kuten SMS-kyselyt (Short Message Service), Telnet ja ohjelmoitavat I/O-portit. SMS-ominaisuudella voidaan laitteelta kysyä tietoja tekstiviestien avulla. 3G-liittymän puhelinnumeroon lähetetään tekstiviesti, jolla voidaan kysyä joko muodostetun verkon tietoja tai käynnistää laite uudelleen. Laitteiden ominaisuuksissa on myös yhtäläisyyksiä, kuten porttisuodattava palomuuri, VPN-tuki, dynaaminen DNS (Domain Name System) ja SNMP (Simple Network Management Protocol). Laitteiden VPN-tuet eroavat kuitenkin käytettävillä kapselointiprotokollilla, jotka ovat IPSec ja GRE Raven XE:ssä sekä PPTP TeleWell 3G -reitittimessä.

5.2 3G-reitittimien käyttöönotto

Ennen laitteiden varsinaista käyttöönottoa on valittava käytettävä 3G-liittymä operaattorilta. Vaihtoehtoina ovat TeliaSonera, DNA, Elisa, Saunalahti ja TeleFinland. Saunalahti ja TeleFinland ovat Elisan ja TeliaSoneran ns. halpaoperaattoreita, joiden liittymät ovat edullisempia ja enemmän kuluttajille suunnattuja. Hinnoiltaan liittymät ovat 12 – 24 €/kk, jos halutaan vähintään HSDPA-tekniikkaa vastaava maksimisiirtonopeus. Jotkin operaattorit ovat myös asettaneet siirtorajoitukset datalle kuukaudessa. Liittymän valintakriteereitä ovat siis siirtonopeus, mahdollinen siirtorajoitus, liittymän kuuluvuusalue ja hinta.

Valitaan lopulta Saunalahden Nopsa-liittymä, jonka hinta on 13,90 €/kk ja maksimisiirtonopeus alavirtaan on 15 Mbit/s. Yksi olennaisimmista liittymän valintaan vaikuttavista tekijöistä on datan siirron mahdollinen rajoitus, jota ei ole Saunalahden Nopsa-liittymässä. Valitaan Saunalahden kahdesta Nopsa-liittymästä siirtonopeudeltaan hitaampi vaihtoehto, jossa alavirran maksimisiirtonopeus on 15 Mbit/s. Toisena vaihtoehtona olisi Nopsa2-liittymä, jolla voidaan saavuttaa 42 Mbit/s siirtonopeus alavirtaan. Mahdolliseen etäkäyttöön riittää kuitenkin 15 Mbit/s siirtonopeus alavirtaan ja liittymissä on sama siirtonopeus ylävirtaan, jossa käytetään HSUPA-tekniikkaa. Hitaampi Nopsa-liittymä on myös huomattavasti edullisempi vaihtoehto. Liittymän mukana tulee Huawei E367 USB 3G-modeemi, jota tarvitaan TeleWell 3G -reitittimessä. Huawei E367 on HSPA+/HSUPA-modeemi, joka mahdollistaa suuremman alavirran siirtonopeuden TeleWell 3G -reitittimessä kuin Raven XE:llä, jonka sisäinen 3G-tekniikka mahdollistaa ainoastaan HSDPA- ja HSUPA-tekniikat.

Liittymän USIM-kortti asetetaan siis TeleWell 3G -reitittimessä käytettävään 3G-modeemiin, kun taas Raven XE:ssä USIM-kortti asetetaan laitteen sisältä löytyvään korttipaikkaan. Molemmat laitteet otetaan käyttöön selaimella, kun USIM-kortti tai 3G-modeemi on tietokoneen lisäksi kytkettynä laitteessa. Raven XE:n käyttöönotto tapahtuu kirjautumisen jälkeen WAN/Cellular-välilehdestä. Käyttöönotossa olennaisin arvo on APN (Access Point Name), joka on operaattorikohtainen liityntäpisteen nimi 3G-yhteydelle. Soneralle, Elisalle ja DNA:lle APN on **internet**, kun taas Saunalahdelle se on **internet.saunalahti**. Muita käyttöönoton

olennaisia perusasetuksia ovat keepalive IP address ja pin-koodin määrittely, jos se on käytössä. Keepalive IP address -asetuksen avulla Raven XE määrittelee, onko Internet-yhteys käytettävissä. Raven XE:n yksi olennaisimmista ominaisuuksista etähallinnassa on **Network watch dog** -ominaisuus, jonka asetukset määrittelemällä voidaan asettaa aika, jossa Raven XE käynnistyy uudelleen Internet-yhteyden puuttuessa. **Network watch dog** -ominaisuuden ajaksi määritellään 15, joka vastaa 15 minuuttia. Yksityiskohtaiset Raven XE:n käyttöönotto-ohjeet löytyvät liitteestä 1.

Kuluttajille suunnatun TeleWell 3G -reitittimen käyttöönotto on pyritty tekemään helpommaksi ohjatun käyttöönoton avulla. Ohjatulla käyttöönotolla asetetaan laitteen järjestelmänvalvojan salasana sekä ulkoverkon ja WLAN-verkon asetukset. Ulkoverkon asetuksissa määritellään mm. APN ja PIN-koodi. Ohjattu käyttöönotto ei kuitenkaan riitä, vaan on asetettava myös 3G-modeemi- ja operaattorikohtaisia asetuksia. Ohjatun käyttöönoton jälkeen on määriteltävä 3G-modeemia vastaava AT-komento, joka pakottaa 3G-verkon käytön. AT-komennoilla voidaan siis ohjata 3G-modeemeja halutuilla tavoilla. Huawei 3G-modeemeille käytetään komentoa **AT^SYSCFG=14,2,3fffffff,1,2**. Lisäksi, jos operaattorina on Saunalahti, on käytettävä CHAP-autentikointia. Yksityiskohtaiset TeleWell 3G -reitittimen käyttöönotto-ohjeet löytyvät liitteestä 6.

5.3 Lisäantennien käyttö

Työssä on käytettävissä 2 kpl Raven XE:n pienitehoisia, n. 3 dBi:n ympärisäteileviä antenneja ja yksi 11 dBi:n jagiantenni, joka toimii 800 – 1000 MHz:n ja 1700 – 2170 MHz:n taajuusalueilla. Antennityypeiksi valitaan ympärisäteilevä ja suunta-antenni, sillä kyseiset antennityypit ovat yleisesti käytettyjä ja eri antennityyppien soveltuvuutta voidaan verrata toisiinsa. Tarkoituksena on testata ympärisäteilevien antennien ja suunta-antennin vaikutusta vastaanotettuun signaalin voimakkuuteen RSSI. Testataan myös Raven XE:n Rx Diversity -ominaisuuden vaikutus RSSI:hin. Testauksessa käytetään Raven XE:tä ja MDMA-ohjelmistoa (Mobile Data Monitoring Application). MDMA:ta käytetään TeleWell 3G -reitittimen sijaan, sillä reititin ei näytä tarkkaa RSSI-arvoa signaalin voimakkuutena käyttöliit-

tymässään. MDMA on mobiiliverkon analysointiin ja antennimittauksiin tehty työkalu, jonka signaalinäyttö on monia 3G-laitteita tarkempi ja ohjelmisto reagoi hieman nopeammin signaalin vaihteluihin (MDMA 2010).

Aloitetaan antennien testaus etsimällä lähimmät tukiasemat. Mittaukset tehdään kaupunkiseudulla, joten alueelta löytyy useita tukiasemia. Karkeita tukiasemien sijainteja löytyy erilaisista Internetin tukiasematietokannoista, mutta tarkka sijainti tarkistetaan Kansalaisen Karttapaikka -palvelusta. Lähistöltä löytyy useita mahdollisia tukiasemia 1,3 – 5,0 km:n etäisyydellä. Näkyvyydeltään mahdollisimman esteetön tukiasema sijaitsee arvioidusti 1,5 km:n päässä mittauspisteestä. Vaihtoehtoisia tukiasemia sijaitsee myös n. 2,5 km:n päässä, mutta niihin on huomattavasti heikompi näkyvyys. Mittauspiste sijaitsee rakennuksen vieressä n. 5 metrin korkeudessa, joten esteettömimmät näkyvyydet tukiasemiin ovat ainoastaan tietyssä kulmassa mittauspisteestä.

Mittaukset aloitetaan, kun mahdollisten tukiasemien sijainteja on tarkasteltu. Jagiantenni suunnataan MDMA-ohjelmistolla ja käytetään Huawei E367-modeemia. Yksittäisellä antennilla tehtävät mittaukset suoritetaan MDMA-ohjelmistolla, kun taas Rx Diversity -ominaisuuden mittaus on tehtävä Raven XE:llä. MDMA-ohjelmistolla suoritettavat mittaukset tehdään tietokoneella, johon 3G-modeemi liitetään suoraan. Jagiantennin SMA-liitin liitetään modeemiin erillisellä liitäntäkaapelilla. Huomioidaan, että liitäntäkaapeli vaimentaa signaalia, mikä vaikuttaa 3G-modeemilla tai TeleWell 3G -reitittimellä muodostettuun 3G-yhteyteen. Raven XE voidaan puolestaan kytkeä suoraan jagiantennin liittimeen. MDMA-ohjelmistossa olennaisia termejä ovat RSSI ja Cell id, joka on tukiaseman solutunnus. Muita ohjelmistossa näkyviä arvoja ovat MCC (Mobile Country Code), MNC (Mobile Network Code) ja LAC (Location Are Code), jotka eivät kuitenkaan muutu, jos operaattori ja mittausalue pysyvät samana. MCC on maakohtainen koodi, joka on Suomessa 244. MNC on operaattorikohtainen koodi, joka on Elisan 3G-verkossa 05. LAC kertoo, millä alueella 3G-verkossa ollaan tällä hetkellä. LAC voi siis muuttua, jos mittauspiste siirrettäisiin toiselle kaupunkiseudulle.

Jagiantennia suuntaamalla löytyy 2 mahdollista tukiasemaa, joiden etäisyydet ovat mittauspisteestä arvioidusti 1,5 – 5,0 km:n välillä. Suuntamittauksissa otetaan tasaisin välein mittausotoksia n. 130 asteen kulman mukaisella alueella, jossa näkyvyys on mahdollisimman esteetön. Suunta-antennia siis käännetään asteittain tasaisin välein, joten ensimmäisen ja viimeisen mittausotoksen suunnat ovat mahdollisimman kaukana toisistaan. Taulukkoon 5 on lueteltu 68 mittausotosta eri suunnista, joissa RSSI on mitattu MDMA-ohjelmistolla. Jokaiseen otokseen on myös mitattu keskimääräinen latenssi.

TAULUKKO 5. Jagiantennin suuntamittaukset MDMA-ohjelmistolla

Otos	Cell ID	RSSI (dBm)	Latenssi (AVG ms)
1	14692	-71	86
2	27829	-67	173
3	14692	-69	160
4	14692	-69	258
5	14692	-67	296
6	14692	-69	102
7	14692	-75	354
8	27829	-73	153
9	27829	-75	98
10	14692	-73	95
11	14692	-71	98
12	14692	-71	78
13	14692	-71	255
14	14692	-71	83
15	14692	-69	150
16	14692	-69	73
17	14692	-73	366
18	27829	-75	315
19	14692	-71	162
20	27829	-69	91
21	14692	-77	161
22	14692	-75	268
23	27829	-73	244
24	14692	-73	313
25	27829	-71	346
26	27829	-69	284
27	14692	-69	243
28	27829	-75	268
29	14692	-69	104
30	27829	-71	157
31	27829	-73	369
32	14692	-71	282
33	14692	-69	125
34	14692	-71	331

Otos	Cell ID	RSSI (dBm)	Latenssi (AVG ms)
35	14692	-71	194
36	14692	-71	204
37	14692	-71	228
38	27829	-71	122
39	14692	-69	87
40	14692	-71	78
41	14692	-73	200
42	27829	-69	257
43	27829	-71	261
44	14692	-71	88
45	14692	-71	139
46	27829	-71	111
47	27829	-71	326
48	27829	-73	183
49	27829	-71	155
50	14692	-73	217
51	14692	-69	196
52	14692	-69	102
53	27829	-71	311
54	14692	-69	99
55	14692	-67	95
56	14692	-69	150
57	14692	-71	177
58	14692	-69	68
59	14692	-71	212
60	14692	-67	75
61	14692	-69	67
62	14692	-65	97
63	14692	-69	82
64	14692	-69	155
65	14692	-67	107
66	14692	-69	117
67	14692	-67	78
68	14692	-73	185

Huomataan, että solutunnuksien 27829 ja 14692 tukiasemiin saadaan yhteys useista eri suunnista. Cell id-tunnuksien lukumääristä huomioidaan, että tukiasemaan 14692 on saadaan enemmän mittausotoksia. Mittausotoksien lukumäärä

tukiasemaa kohden kertoo tukiasemien etäisyydestä ja näkyvyydestä. Tukiasemaan 14692 os siis esteettömin näkyvyys ja tukiasema sijaitsee mahdollisesti lähempänä kuin muut tukiasemat. Huomataan, että mittausotoksien 1 – 53 välillä tukiasemat vaihtelevat. Tämä kertoo mahdollisesti, että kyseisellä välillä tukiasemien kuuluvuusalueet risteytyvät. Mittausotoksien 54 – 68 välillä ei puolestaan tapahdu muutoksia tukiasemassa. Tukiaseman RSSI ja latenssi ovat myös selvästi parempia kyseisellä välillä. Tarkastamalla mittausotoksien 54 - 68 suunta ja vertaamalla sitä Kansalaisen Karttapaikka -palvelusta löydettyyn mahdollisen tukiaseman sijaintiin, voidaan todeta, että kyseessä on sama tukiasema. Suuntaamalla jagiantenni tukiaseman 14692 suuntaan, saadaan hienosäätämällä signaali voimakkaammaksi -65 dBi:n tasolle. Huomioidaan myös, että mitattu keskimääräinen latenssi ei ole suoraan verrannollinen mitattuun RSSI-arvoon. Heikolla signaalin voimakkuudella voidaan saavuttaa alhainen latenssi, ja vastaavasti vahva signaalin voimakkuus ei takaa alhaista latenssia. Latenssin avulla voidaan arvioida signaalin luotettavuutta ja mahdollisia häiriötekijöitä tukiaseman ja mittauspisteen välillä. Huomataan mittausotoksista 54 - 68, että latenssi on keskimääräisesti alhaisempi ja vakaampi, mitä tarkemmin antenni suunnataan tukiasemaan 14692. Tämä vahvistaa käsitystä tukiaseman sijainnista.

Kaupunkiseuduilla käytetään yleisesti ympärisäteileviä lisäantenneja tukiasemien määrän ja lyhyen etäisyyden vuoksi. Mitataan seuraavaksi RSSI pienitehoisella ympärisäteilevällä antennilla. Ympärisäteilevää antennia mitatessa tarvitaan ainoastaan yksi mittausotos, joka on -65 dBm:ää tukiasemalle 14692. Signaalinvoimakkuudeksi saadaan siis sama arvo kuin suunnatulla 11 dBi:n jagiantennilla. On kuitenkin otettava huomioon antennikaapeleiden pituudet, jotka vaikuttavat myös antennien lopullisiin vahvistuksiin. Voidaan päätellä, että kattavan 3G-verkon omaavalla kaupunkiseudulla ei saada suunta-antenneista tarvittavaa hyötyä, ja voidaan käyttää pienempitehoisia ja yleisesti edullisempia ympärisäteileviä antenneja.

3G-verkossa toimiva RSSI on yleisesti -60 dBm:n ja -100 dBm:n väliltä. Mitä lähempänä RSSI on -100 dBm:ää, sitä enemmän tapahtuu datan häviötä radiolinkillä. 3G-yhteys on luotettava jopa -80 dBm:n RSSI:llä. Ympärisäteilevällä antennilla mitattu -65 dBm:n RSSI on siis suhteellisen voimakas ja sietokykyinen sig-

naali. Huomioidaan, että mittaus on tehty ulkotilassa ja yhdellä ympärisäteilevällä antennilla. Raven XE:ssä on mahdollisuus käyttää kahta antennia Rx Diversity -ominaisuudella, jolloin RSSI:tä on mahdollista parantaa. Signaalin ollessa voimakas ulkotilassa simuloidaan heikompi signaali tekemällä Rx Diversity -mittaus sisätilassa, jotta olisi mahdollista huomata selkeämpi RSSI:n ero Rx Diversity -ominaisuutta käyttämällä. Kahden antennin käytössä antennit on asetettava mahdollisimman etäälle toisistaan ja samalle korkeudelle, jotta saataisiin mahdollisimman suuri hyöty Rx Diversity -ominaisuudella. Ympärisäteilevillä antenneilla tehdyssä Rx Diversity -mittauksessa saadaan signaalin voimakkuudeksi -76 dBm:ää kahdella antennilla ja -79 dBm:ää yhdellä antennilla sisätilassa. Tuloksista huomataan selkeä ero. Kuviosta 10 nähdään Raven XE:n käyttöliittymästä saadut mittaustulokset kahdella antennilla. Huomataan myös kuvassa näkyvä EC/IO-arvo, jolla kuvataan SNR:n tavoin signaalin laatua. Mitä lähempänä EC/IO-arvo on 0 dBm:ää, sitä parempi signaalin laatu on.

AT Phone Number	
AT IP Address	85.76.101.111
AT Network State	Network Ready
AT RSSI (dBm)	-76
AT Cell Info	Cell Info: BSIC: 0 TCH: 10588 RSSI: -76 LAC: 25300 CellID: 27829
AT Current Network Operator	elisa, 24405
AT Network Service Type	HSPA
AT ALEOS Software Version	H2295E_4.0.6.001 May 4 2010
AT EC/IO (dB)	-2.5
AT Channel	10588
WAN/Cellular Bytes Sent	350862
WAN/Cellular Bytes Rcvd	317991
AT Device Name	dd-c

KUVIO 10. Rx Diversity -mittaus Raven XE:en käyttöliittymällä

5.4 Tietoturvan käyttöönotto

Laitteiden olennaisimmat tietoturvaominaisuudet koostuvat suodattavista palomuuritekniikoista ja VPN-tuesta. Molemmissa laitteissa on portti-, IP- ja MAC-suodattavat (Media Access Control) palomuurio minaisuudet, joilla voidaan halutessa suodattaa sisä- ja ulkoverkosta tulevaa liikennettä. Määritetyillä suodatussäännöillä voidaan joko sallia tai estää kaikki, paitsi sääntöjen mukainen liikenne. TeleWell 3G -reitittimessä on myös verkkotunnus- ja URL-suodatukset (Uniform Resource Locator), jotka estävät määriteltyjen sivustojen selaamisen sisäverkosta.

Tarvittaessa laitteissa voidaan myös määritellä DMZ-kohde (Demilitarized Zone), joka ei ole suojeltu palomuurilla. Palomuurilla voidaan myös estää kaikki liikenne ulkoverkosta, jos etähallittavalle laitteella ei tarvitse olla muita yhteyksiä VPN-tunnelin lisäksi. Laitteet eroavat VPN-ominaisuuksiltaan huomattavasti. TeleWell 3G -reitittimessä käytetään PPTP:tä joko asiakkaana tai palvelimena. Raven XE puolestaan tukee IPSec- ja GRE-tunneleita.

TeleWell 3G-reitittimessä tietoturva-asetukset määritellään turvallisuusasetukset-välilehdestä. Suodattavista ominaisuuksista MAC-, verkkotunnus- ja URL-suodatukset kohdistuvat sisäverkon laitteille. Pakettisuodatus on siis laitteen varsinainen palomuuriominaisuus, jolla pystytään estämään ulko- ja sisäverkon välinen liikenne porttien ja IP-osoitteiden mukaan. Laitteen pakettisuodatukseen voidaan ainoastaan määritellä 8 sääntöä molempiin suuntiin. Huomioidaan myös, että saapuvien pakettien suodatus vaikuttaa vain DMZ-kohteeseen ja porttiohjauksiin. Pakettisuodatussääntöihin on määriteltävä kohteen ja lähteen IP-osoite sekä portti. Reitittimeen voidaan lisäksi sallia etähallinta halutusta ulkoverkon IP-osoitteesta. Raven XE:n portti-, IP- ja MAC-suodatukset otetaan käyttöön security-välilehdestä. TeleWell 3G -reitittimen tavoin Raven XE:ssä määritellään porttisuodatukset joko sisä- tai ulkoverkkoon päin. Porttisuodatuksien määrää ei ole rajoitettu kuten TeleWell 3G -reitittimessä. Huomataan että, Raven XE:n porttisuodatuksessä määritellään ainoastaan portit, jotka estetään. TeleWell 3G -reitittimessä voidaan puolestaan määritellä lähteen ja kohteen IP-osoitteet porttien lisäksi. Raven XE:n IP-suodatus tehdään erikseen sisä- tai ulkoverkkoon päin Trusted IPs -välilehdistä.

TeleWell 3G -reitittimen VPN voidaan toteuttaa joko PPTP-asiakkaana tai PPTP-palvelimena. Toteutukset eroavat VPN-tunnelin yhteyden muodostuksessa ja lopullisen IP-osoitteen jakamisessa. Jos yhteys halutaan muodostaa ulkoverkosta 3G-reitittimeen, on reitittimestä tehtävä PPTP-palvelin. Tällöin PPTP-palvelimeen määritellään käyttäjätili, käyttäjälle jaettava IP-osoite, autentikointiprotokolla ja mahdollinen salaus. PPTP-palvelimeen voidaan luoda 5 samanaikaista käyttäjätiliä, jotka vastaavat samanaikaisia tunneleita. PPTP-palvelimeen otetaan yhteys esimerkiksi Windows 7 -käyttöjärjestelmän VPN-asiakkaalla, jolle on määritelty palvelimelle tehdyn käyttäjätilin tiedot. Vaihtoehtoisesti reititin voidaan asettaa

PPTP-asiakkaaksi, jolloin VPN-yhteys muodostetaan reitittimellä ulkoverkon PPTP-palvelimeen. Tällöin PPTP-palvelimena voi toimia esimerkiksi Windows 7 -käyttöjärjestelmän VPN-palvelin tai erillinen VPN-reititin.

Raven XE:n VPN-tuki otetaan käyttöön VPN-välilehdestä, jossa on mahdollista luoda 5 samanaikaista VPN-tunnelia joko IPSec:llä tai GRE:llä. Työssä käsitellään tarkemmin IPSec-tunnelin luontia, sillä se on huomattavasti tietoturvallisempi ja yleisemmin käytetty menetelmä kuin GRE. PPTP:n sijaan IPSec soveltuu paremmin kahden lähiverkon yhdistämiseen, jolloin VPN-tunneli luodaan kahden VPN-yhdyskäytävän välille. Olennaisimmat IPSec-tunnelille määriteltävät asetukset ovat vastaanottajan julkinen osoite, salausavain, neuvottelumenetelmä, VPN-laitteille määriteltävät aliverkko-osoitteet ja IKE-vaiheiden parametrit. Neuvottelumenetelmäksi voidaan valita joko aggressiivinen- tai main-moodi, jotka määrittelevät IKE-vaiheen 1 toiminnan. IKE-vaiheiden parametrejä ovat salausalgoritmi, autentikointialgoritmi, avainryhmä ja SA-elinaika, jotka määritellään molemmille IKE-vaiheille. Raven XE:ssä IKE-vaiheet 1 ja 2 ovat nimetty IKE- ja IPSec-vaiheiksi. Salausavaimen ja IKE-parametrien on oltava samoja VPN-tunnelin molemmissa VPN-yhdyskäytävissä. Laitteeseen on myös mahdollista sallia **out of band**, jolloin Internetiä voidaan käyttää normaalisti Raven XE:n lähiverkosta, vaikka VPN-tunneli olisi kytketty. Tietoturvan kannalta out of band -ominaisuuden tulisi olla kuitenkin estettynä, jos etähallittavan laitteen ei tarvitse olla yhteydessä Internetiin. Tarkemmin Raven XE:n VPN-neuvottelua voidaan tarkastella log-välilehdestä, joka on hyödyllinen esimerkiksi vikatilanteissa. Kuviosta 11 nähdään onnistunut IPSec-neuvottelu Raven XE:n log-ominaisuudella tarkasteltuna. Yksityiskohtaiset TeleWell 3G -reitittimen ja Raven XE:n perustietoturvan käyttöönotto-ohjeet löytyvät liitteistä 2 ja 7.

KUVIO 11. IPSec-neuvottelu Raven XE:n VPN-lokista

5.5 Etähallinta

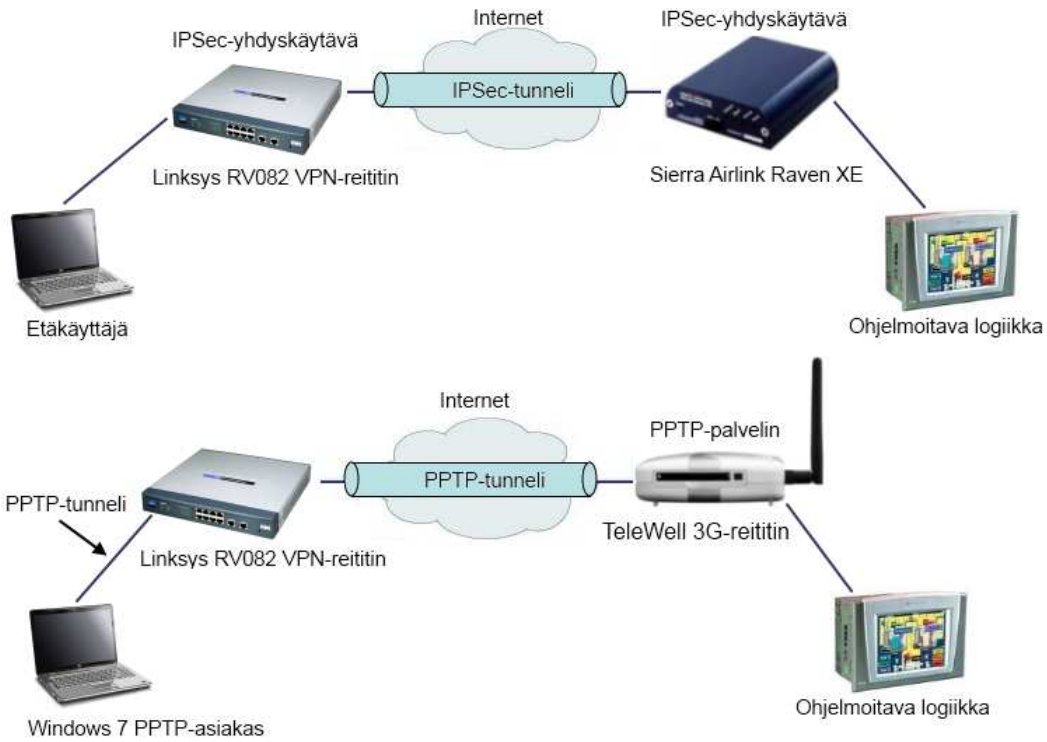
Tässä työssä on tarkoitus tutkia etähallintamahdollisuuksia edellä mainituilla laitteilla. Yksi mahdollisista laitteiden käyttökohteista tulee olemaan erilaisten automaatiologiikoiden etähallinta. Logiikan etähallinnalle luodaan 3G-yhteys ja tarkastellaan VPN:n vaikutusta etähallintaan. Työssä on käytössä Unitronics ohjelmoitava logiikka, jolle on oma Remote Operator -etähallintaohjelmisto. Logiikka käyttää etähallintaan valmistajan omaa PCOM-protokollaa. VPN-tunneleiden muodostuksessa käytetään Linksys RV082 VPN-reititintä ja Windows 7 -käyttöjärjestelmän VPN-asiakasta.

Yksi olennaisimmista etähallintaan liittyvistä ominaisuuksista 3G-yhteydessä on dynaaminen DNS -palvelu. 3G-verkossa päätelaitteen IP-osoite on dynaaminen, jolloin IP-osoite vaihtuu jatkuvasti. Tämä aiheuttaa etähallinnassa ongelman, sillä päätelaitteen IP-osoite on tiedettävä, jotta voitaisiin muodostaa yhteys. Etähallittava kohde voi olla myös kaukainen ja miehittämätön, jolloin IP-osoitteen tarkistus kohteessa on hankalaa. Tällöin on käytettävä esimerkiksi dynaamista DNS-palvelua, joka määrittelee halutun verkkotunnuksen vaihtuvalle IP-osoitteelle. Yleisesti on rekisteröidyttävä johonkin dynaamisen DNS:n tarjoavaan palveluun,

kuten DynDNS (www.dyndns.org) tai suomalainen dy.fi (www.dy.fi). Raven XE:ssä voidaan kuitenkin käyttää Sierran omaa dynaamista DNS-palvelua. Laitteelle määritellään nimi, jota käytetään dynaamisen DNS-palvelun luoman verkkotunnuksen etuliitteenä. Esimerkiksi laitteen nimi **dd-c** muodostaa verkkotunnuksen **dd-c.eairlink.com**. TeleWell 3G -reitittimessä on puolestaan rekisteröidyttävä erilliseen palveluun, joka tarjoaa dynaamisen DNS:n. Rekisteröidytään siis dy.fi-palveluun. Määritellään palveluun haluttu verkkotunnuksen etuliite **3g-testi**, jolloin verkkotunnukseksi muodostuu **3g-testi.dy.fi**. Laitteiden tarkat dynaamisen DNS-ominaisuuden käyttöohjeet löytyvät liitteistä 5 ja 9.

Logiikan etähallinta voidaan toteuttaa joko VPN-tunnelilla tai ilman tunnelia käyttämällä 3G-reitittimen porttiohjausta etähallittavaan laitteeseen. Toteutettavat IPSec- ja PPTP-tunnelit eroavat toisistaan tunnelin päätepisteillä. IPSec-tunneli tehdään Linksys rv082 VPN-reitittimen ja Raven XE:n välille. Laitteisiin määritetään samat salausavaimet ja IKE-vaiheiden parametrit. Asetetaan myös Raven XE:ssä **keep tunnel alive** -vaihtoehtoon **yes**, jolloin Raven XE muodostaa VPN-tunnelin automaattisesti. Yhteyden muodostuksessa havaitaan kuitenkin ongelma. IPSec-tunneli on asetettava aggressive mode -tilaan, sillä Linksys-reititin toimii main mode -tilassa ainoastaan Microsoftin VPN-asiakkaiden kanssa.

TeleWell 3G -reitittimessä on mahdollisuus toteuttaa VPN-tunneli joko asiakkaana tai palvelimena. Reitittimen PPTP-asiakas -ominaisuus soveltuu paremmin etähallintaan, sillä asiakkaana reititin muodostaa yhteyden. Tällöin VPN-tunneli muodostuu automaattisesti ja dynaamista DNS-palvelua ei ole välttämätöntä käyttää, sillä PPTP-palvelimen ei tarvitse tietää 3G-reitittimen julkista IP-osoitetta. Pakettien katoamisena ilmenevien yhteensopivuusongelmien vuoksi PPTP-tunneli toteutetaan kuitenkin Windows 7 VPN-asiakkaalla, jolloin TeleWell 3G-reititin asetetaan PPTP-palvelimeksi. Tällöin PPTP-palvelimessa dynaaminen DNS-ominaisuus on tarpeellinen, sillä VPN-asiakkaan on tiedettävä 3G-reitittimen IP-osoite tai verkkotunnus. Käytetään PPTP-palvelimen asetuksissa Microsoft:n MS_CHAPv2-autentikointiprotokollaa ja MPPE-salausta (Microsoft Point-to-Point Encryption) 128-bittisellä avaimella. Kuviossa 12 verrataan laitteiden VPN-toteutuksia. Huomioidaan, että PPTP-tunneli kulkee Linksys-reitittimen läpi.



KUVIO 12. IPSec- ja PPTP-toteutukset

Vaihtoehtoisesti etähallinta voidaan myös toteuttaa ilman VPN-tunnelia porttiohjaamalla 3G-reitittimelle tuleva liikenne lähiverkkoon etähallittavalle laitteelle. Tällöin on käytettävä 3G-reitittimen julkista IP-osoitetta, joten dynaaminen DNS tarpeellinen ominaisuus tässäkin tapauksessa. Laitteiden porttiohjaussäännöissä on määriteltävä julkinen portti, etähallittavan laitteen yksityinen IP-osoite ja yksityinen portti. Etähallinnassa käytettävä Ohjelmoitava logiikka käyttää porttia 20256, joka määritellään julkiseksi ja yksityiseksi portiksi. Ohjelmoitavan logiikan yksityinen IP-osoite on määriteltävä käsin, sillä logiikan ohjelmisto tukee ainoastaan manuaalisesti asetettua IP-osoitetta. Tarkat 3G-reitittimien VPN- ja porttiohjausohjeet löytyvät liitteistä 3 - 4 ja 8 - 9. Linksys VPN-reitittimen ja Windows 7 VPN-asiakkaan tarkat konfiguraatio-ohjeet löytyvät liitteistä 10 - 11.

Toteutetaan etähallinta pääasiassa VPN-tunnelilla, mutta tehdään myös vaihtoehtoinen porttiohjaus, jolloin etähallinta onnistuu myös VPN-yhdyskäytävän tai VPN-asiakkaan puuttuessa. Mahdollistetaan myös 3G-reitittimen etähallinta ulkoverkosta, jotta reitittimen asetuksia voidaan muuttaa tarvittaessa. Porttiohjaus ja 3G-reitittimen etähallinta turvataan sallimalla yhteys vain siitä IP-osoitteesta, josta etähallitaan. Määritellään siis TeleWell 3G -reitittimestä etähallinta käyttöön halu-

tusta kiinteästä IP-osoitteesta tai isäntänimestä, jos sellainen on käytössä. Sallitaan myös yhteydet vain tietystä IP-osoitteesta saapuvien pakettien suodatuksella. Estetään siis kaikki muu, paitsi määritellyn säännön mukainen liikenne. Otetaan 3G-reitittimen etähallinta myös käyttöön Raven XE:stä, jossa ei voida kuitenkaan määritellä etähallinnalle tiettyä IP-osoitetta. Voidaan kuitenkin sallia vain tietyt IP-osoitteet ulkoverkosta Trusted IPs -ominaisuudella. Laitteisiin ei siis tarvitse määritellä kuin yksi sääntö, jos sallitaan kaikki liikenne etähallittavan laitteen ja käyttäjän välillä. Vaihtoehtoisesti Raven XE:n etähallinta voidaan sallia vain tietyistä MAC-osoitteista, jos etähallinta halutaan mahdollistaa tietokoneen mukaan.

Antennimittauksien mukaan etähallintaan muodostetulla 3G-yhteydellä saavutetaan parhaimmillaan 60 - 100 ms:n latenssi, mutta ajoittain tapahtuu pakettien häviötä ja latenssi kasvaa yli 300 ms:iin. Logiikan etähallinnassa käytettyä ohjelmistoa ja protokollaa ei ole suunniteltu langattomaan etäkäyttöön, joten latenssin on oltava mahdollisimman alhainen. Logiikan etähallinta toimii 60 – 150 ms:n latenssilla, mutta korkeimmilla latensseilla Remote Operator-ohjelmiston etähallintayhteys on epävakaa. Ajoittainen pakettien häviö tai suuri väliaikanen latenssi voi myös katkaista Remote Operator -etäyhteyden. VPN-tunnelin käyttö ei vaikuta suuresti latenssiin. Vertaamalla IPSec- ja PPTP-toteutuksien latensseja saadaan IPSec:stä n. 20 ms nopeampi kuin PPTP. IPSec:n latenssi on puolestaan n. 10 ms korkeampi kuin normaalilla yhteydellä, jossa ei käytetä VPN:ää. VPN:n vaikutus latenssiin on siis minimaalinen, eikä ero ole selkeä käyttäjälle.

Testien ja laitteiden ominaisuuksien perusteella valitaan etähallintaan optimaalisin 3G-reititin. Laitteiden ominaisuuksista huomataan, että Raven XE soveltuu paremmin etähallintaan. Varsinkin Raven XE:n network watch dog -ominaisuus on tärkeä etähallinnassa, jos etähallittava kohde on miehittämätön ja kaukana etähallitsijasta. Raven XE on myös tietoturvallisempi IPSec-yhteyden ansiosta. Toisaalta, etähallitsijan IPSec-yhdyskäytävän puuttuessa VPN-tunneli on muodostettava TeleWell 3G -reitittimellä, jonka PPTP-palvelimeen voidaan muodostaa yhteys Windows 7:n VPN-asiakkaalla. TeleWell 3G -reitittimen käyttöönotto on pyritty tekemään yksinkertaisemmaksi, mutta erilaiset TeleWell 3G -reitittimessä tehtävät operaattori- ja modeemikorttikohtaiset asetukset sekä erillisesti hankittava dynaaminen DNS-palvelu tekevät Raven XE:n käyttöönotosta yksinkertaisempaa. Ra-

ven XE:hen suoraan liitettävät antennit parantavat signaalin laatua ja vähentävät käytettävien komponenttien määrää verrattuna TeleWell 3G -reitittimeen, jossa on käytettävä erillistä antennin liitäntäkaapelia. Raven XE:n kestävyys tekee laitteesta myös paremman vaihtoehdon mahdolliseen ulkokäyttöön. Raven XE on suositeltava vaihtoehto laitteiden etähallintaan, kun taas TeleWell 3G -reititin soveltuu parhaiten esimerkiksi väliaikaisen Internet-yhteyden tarjoamiseen työmaalla.

6 YHTEENVETO

Tässä opinnäytetyössä tutkittiin kahden 3G -reitittimen soveltuvuutta ja käyttöönottoa etähallintaratkaisuun, joka mahdollisesti toteutetaan ohjelmoitavalle logiikalle. Opinnäytetyössä tutkittiin myös ympärisäteilevän ja suunta-antennin vaikutusta 3G-yhteyteen. Etähallinnassa keskityttiin erityisesti tietoturvallisuuteen, joka saavutettiin tehokkaimmin VPN-tunnelia käyttämällä.

3G-reitittimien tutkiminen aloitettiin vertailemalla laitteiden ominaisuuksia. Ominaisuuksia vertailemalla huomattiin selvästi laitteille suunnitellut käyttötarkoitukset, jotka jaettiin kuluttaja- ja teollisuuskäyttöön. Ominaisuuksien perusteella voitiin jo todeta, että Raven XE soveltuu huomattavasti paremmin etähallintaan, johon se on myös suunniteltu. TeleWell 3G -reititin puolestaan keskittyy 3G-yhteyden jakamiseen lähiverkkoon, mikä tekee siitä käytännöllisemmän kuluttajille.

Antennien käytöstä ja signaalin mittaamisesta voitiin todeta, että suunta-antennin käyttö kaupunkiseudulla ei ole yleisesti tarpeellista, vaikka suunta-antennilla voidaan varmistaa signaali haluttuun tukiasemaan. Ympärisäteilevällä antennilla on mahdollista saada suunnattua suunta-antennia vastaava signaali, sillä yleisesti kaupunkiseudut ovat hyvin katettuja 3G-kuuluvuudeltaan. Opinnäytetyössä tehdyt antennimittaukset olisi voitu tehdä kattavammin vertaamalla saatuja tuloksia tukiasemien kuuluvuusalueiden rajalla tehtyihin mittauksiin. Tällöin suunta-antennin tuoma hyöty olisi tullut paremmin esille.

Reitittimien etähallinnan mahdollistaminen onnistui ongelmitta. Huomattiin, että Raven XE:ssä korostuu etähallinta network watch dog -ominaisuudella ja valmistajan omalla DNS-palvelulla. Tietoturvan käyttöönotossa ilmeni joitain yhteensopivuusongelmia käytettävän VPN-reitittimen kanssa, mutta VPN-tunneli saatiin lopulta muodostettua. TeleWell 3G -reitittimessä ei saatu PPTP-asiakastoimintoa toimimaan halutulla tavalla, joten VPN-yhteys ei muodostu automaattisesti. Todetaan, että tietoturvan ja etähallinnan kannalta Raven XE on huomattavasti luotettavampi ratkaisu. Ohjelmoitavan logiikan etähallinta onnistui molemmilla 3G-reitittimillä käyttäen sekä VPN-tunnelia että porttiohjausta.

3G-etähallinnan merkitys yritykselle on suuri, sillä kiinteän Internet-yhteyden saatavuus on rajoitettu monissa tarvittavissa kohteissa. Kiinteän Internet-yhteyden hankinta voi olla myös epäkäytännöllistä varsinkin väliaikaisissa kohteissa. Yrityksen käyttämä suljettu radioverkko ei myöskään sovellu kaikille etähallintatoteutuksille esimerkiksi vähäisen kuuluvuusalueen tai radiomodeemiverkon siirtonopeuden vuoksi. UMTS-verkko takaa huomattavasti nopeamman ja kuuluvuusalueeltaan laajemman ratkaisun. Etähallinnan merkitys ympäristölle on myös huomattava. Vaikka jatkuvaa etähallintaa ei tarvittaisi kohteessa, on laitteita tarvittaessa pystyttävä ohjelmoimaan jollakin tavalla, jolloin laitteen ja toimipisteen välimatkalla syntymiä ajoneuvopäästöjä voidaan vähentää etähallintayhteydellä. Etähallintaan suunniteltu 3G-reititin takaa yhteyden pysyvyyden ja virhetilanteessa yhteyden uudelleen muodostamisen, jolloin toimipisteen ja etähallittavan kohteen välillä ei tarvitse matkustaa.

LÄHTEET

3G ja 4G. 2011. Sonera [viitattu 13.8.2011]. Saatavissa: http://www5.sonera.fi/ohjeet/3G_ja_4G

3G-kuuluvuusalueet. 2011. Sonera [viitattu 13.8.2011]. Saatavissa: http://www.sonera.fi/asiakastuki/puhelin+ja+liittymat/kuuluvuus+ja+nopeuskartta/

3G LTE Tutorial. 2011. Radio-electronics [viitattu 11.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php

3GPP TS 25.101. 2011. 3GPP [viitattu 9.8.2011]. Saatavissa: http://www.3gpp.org/ftp/Specs/archive/25_series/25.101/25101-a20.zip

4G LTE Advanced Tutorial. 2011. Radio-electronics [viitattu 11.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3gpp-4g-imt-lte-advanced-tutorial.php

Antennin valinta. 2011. Siptune [viitattu 14.8.2011]. Saatavissa: http://www.siptune.net/tiki-index.php?page=Antennin+valinta

CHAP. 2000. Searchcio-midmarket [viitattu 10.9.2011]. Saatavissa: http://searchcio-midmarket.techtarget.com/definition/CHAP

DNA 4G. 2011. DNA [viitattu 13.8.2011]. Saatavissa: http://www.dna.fi/YKSITYISILLE/LIIKKUVALAAJAKAISTA/4G-TESTI/Sivut/Default.aspx

DNA Mokkula MC545. 2011. DNA [viitattu 13.8.2011]. Saatavissa: http://www.dna.fi/yksityisille/liikkuvalaajakaista/laitteet/Sivut/mokkulamc545.aspx

Dual Carrier HSPA. 2011. Radio-electronics [viitattu 10.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/dc-dual-carrier-hspa-hsdpa.php

Granlund, K. 2007. Tietoliikenne. Porvoo: WS Bookwell.

HSPA Tutorial. 2011. Radio-electronics [viitattu 10.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/umts-high-speed-packet-access-tutorial.php

Evolved HSPA / HSPA+. 2011. Radio-electronics [viitattu 10.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/evolved-high-speed-packet-access-evolution.php

HSDPA Tutorial. 2011. Radio-electronics [viitattu 10.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/hsdpa-high-speed-downlink-packet-access.php

HSUPA Tutorial. 2011. Radio-electronics [viitattu 10.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/hsupa-high-speed-uplink-packet-access.php

Identify authentication protocols. 2010. Computer networking notes [viitattu 10.9.2011]. Saatavissa: http://computernetworkingnotes.com/n_plus_certifications/protocol.html

IMT-advanced. 2010. ITU [viitattu 11.8.2011]. Saatavissa: http://www.itu.int/ITU-R/index.asp?category=information&rlink=imt-advanced&lang=en

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo: WS Bookwell.

Kuinka suunta-antenni suunnataan kotikonstein?. 2011. 3G-antennit [viitattu 15.8.2011]. Saatavissa: http://www.3g-antennit.fi/news/3/

LTE MIMO System-Level Design. 2009. Agilent Technologies [viitattu 15.8.2011]. Saatavissa: http://www.home.agilent.com/upload/cmc_upload/All/LTE-MIMO-System-Level-Design.pdf?&cc=FI&lc=fin

MDMA. 2010. Siptune [viitattu 20.8.2011]. Saatavissa: http://www.siptune.net/tiki-index.php?page=MDMA

MIMO Formats. 2011. Radio-electronics [viitattu 14.8.2011]. Saatavissa: http://www.radio-electronics.com/info/antennas/mimo/formats-siso-simo-miso-mimo.php

MIMO Technology Tutorial. 2011. Radio-electronics [viitattu 15.8.2011]. Saatavissa: http://www.radio-electronics.com/info/antennas/mimo/multiple-input-multiple-output-technology-tutorial.php

Nettitikku E398. 2011. Saunalahti [viitattu 13.8.2011]. Saatavissa: http://saunalahti.fi/puhelimet/puhelin.php?id=568&type=handsetmodel

Operaattoreiden kuuluvuuskartat. 2011. Siptune [viitattu 12.8.2011]. Saatavissa: http://www.siptune.net/tiki-index.php?page=Operaattoreiden+kuuluvuuskartat

Penttinen, J. 2006. Tietoliikennetekniikka: 3G ja erityisverkot. Helsinki: WSOY.

Radiolupapäätös 18305/730/2006. 2006. Ficora [viitattu 8.8.2011]. Saatavissa: http://www.ficora.fi/attachments/suomimq/5keG9URVc/Paat061031DNAVerkotOy.pdf

Radiolupapäätös 228/702/2009. 2009. Ficora [viitattu 8.8.2011]. Saatavissa: http://www.ficora.fi/attachments/5gAgI20TP/paat2GHz_090417.pdf

Radiolupapäätös 12979/730/2009. 2009. Ficora [viitattu 8.8.2011]. Saatavissa: http://www.ficora.fi/attachments/suomimq/5liUHc7vF/Paat011209Elisa.pdf

RFC 2759. 2000. IETF [viitattu 10.9.2011]. Saatavissa: http://tools.ietf.org/html/rfc2759

Thomas, T. 2005. Verkkojen tietoturva. Helsinki: Edita Prima Oy.

UMTS 3G History. 2011. Radio-electronics [viitattu 4.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/umts/3g-history.php

UMTS Overview. 2002. UMTS World [viitattu 6.8.2011]. Saatavissa: http://www.umtsworld.com/technology/overview.htm

UMTS / WCDMA Network Architecture. 2011. Radio-electronics [viitattu 5.8.2011]. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/umts/umts-wcdma-network-architecture.php

What is Ec/Io. 2011. Telecomhall [viitattu 10.9.2011]. Saatavissa: http://www.telecomhall.com/what-is-ecio-and-ebno.aspx

Yagi. 2011. Radio-electronics [viitattu 14.8.2011]. Saatavissa: http://www.radio-electronics.com/info/antennas/yagi/yagi.php

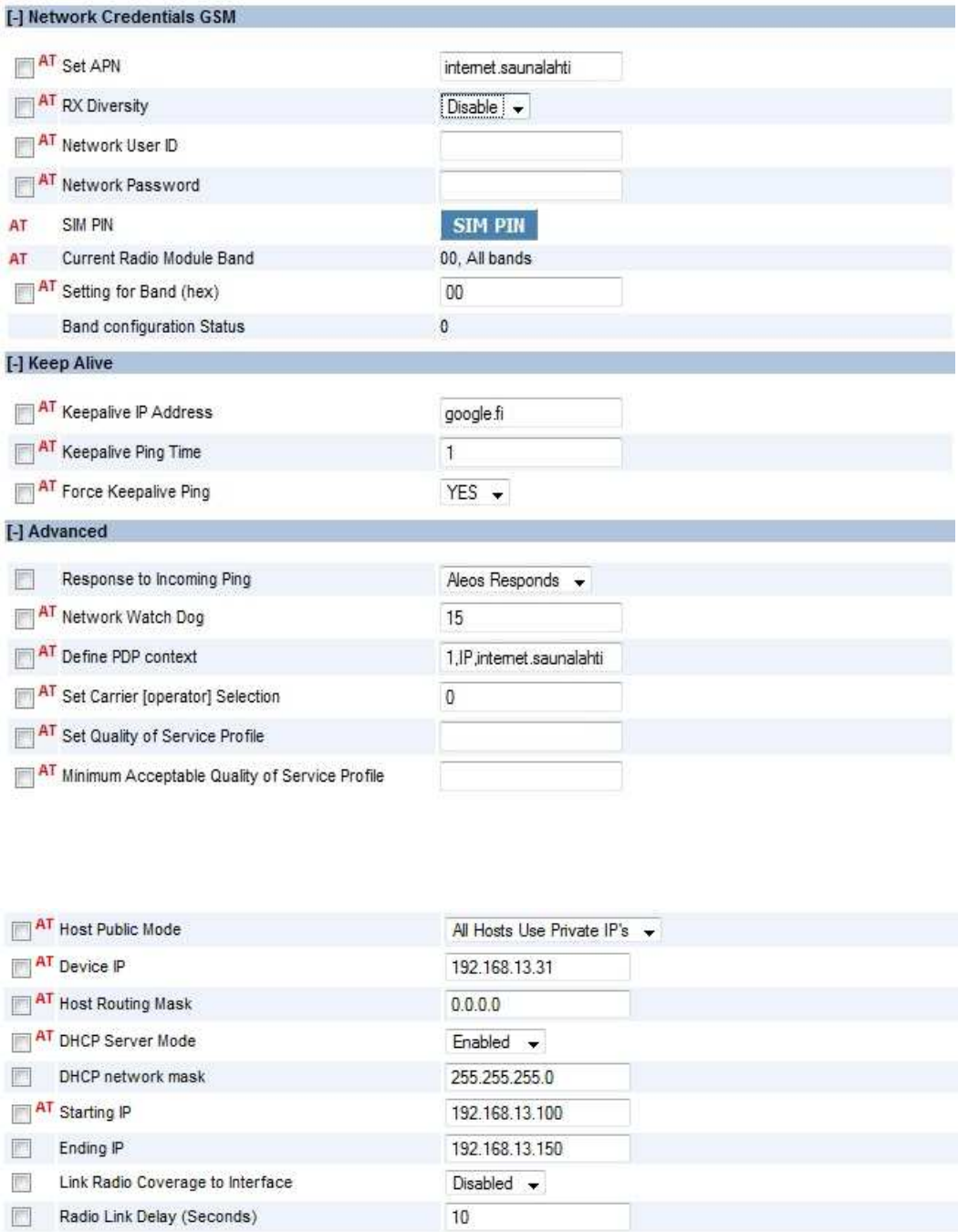
LIITTEET

LIITE 1 1/2

Sierra Airlink Raven XE käyttöönotto-ohje

1. Avataan laite ja asetetaan USIM-kortti laitteen sisällä olevaan korttipaikkaan, joka sijaitsee merkkivalojen puoleisessa päädyssä. On suositeltavaa, että USIM-kortin PIN-koodin kysely on poissa käytöstä. PIN-koodin kysely voidaan poistaa käytöstä matkapuhelimen asetuksista.
2. Kytketään tietokone Rave XE:n ethernet porttiin ja otetaan yhteys laitteeseen selaimella (suosituksena Internet Explorer) osoitteesta **192.168.13.31:9191**. Oletusasetuksien käyttäjänimi ja salasana ovat **user** ja **12345**.
3. Valitaan WAN/Cellular-välilehti, jossa määritellään APN-arvoksi **internet.saunalahti**, jos käytössä on Saunalahden liittymä. Muille liittymille APN-arvo on **internet**.
4. Asetetaan myös Keepalive IP address-arvoksi luotettava web-osoite kuten **google.fi**. Keepalive ping time -arvoksi **1** ja force keepalive ping -arvoksi **YES**.
5. Advanced-kohdassa asetetaan network watch dog -arvoksi **15**.
6. Asetukset tallennetaan valitsemalle **Apply** ja laite on käynnistettävä uudelleen valitsemalla **Reboot**, kun kaikki halutut asetukset on määritelty.
7. LAN-välilehdestä voidaan asettaa ethernet-portti sillattuun tai reititettyyn tilaan valitsemalla haluttu Host public mode -tila. Tässä tapauksessa **All Hosts Use Private IPs**.
8. Laitteen oma IP-osoite voidaan määritellä Device IP -kohdasta. Jaettavat IP-osoitteet voidaan määritellä **starting IP**- ja **ending IP** -kohdista, jos **DHCP server mode** on **enabled**-tilassa.

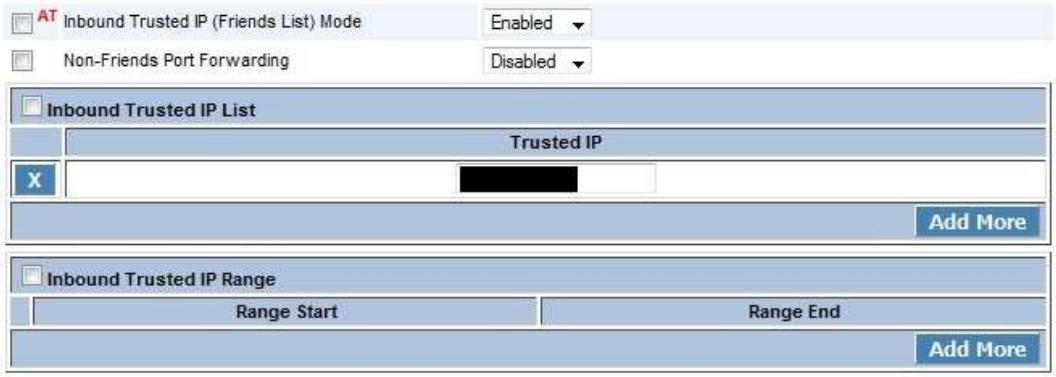
LIITE 1 2/2


[-] Network Credentials GSM
AT Set APN
internet.saunalahti
AT RX Diversity
Disable
AT Network User ID
AT Network Password
AT SIM PIN
SIM PIN
AT Current Radio Module Band
00, All bands
AT Setting for Band (hex)
00
Band configuration Status
0
[-] Keep Alive
AT Keepalive IP Address
google.fi
AT Keepalive Ping Time
1
AT Force Keepalive Ping
YES
[-] Advanced
Response to Incoming Ping
Aleos Responds
AT Network Watch Dog
15
AT Define PDP context
1,IP,internet.saunalahti
AT Set Carrier [operator] Selection
0
AT Set Quality of Service Profile
AT Minimum Acceptable Quality of Service Profile
AT Host Public Mode
All Hosts Use Private IP's
AT Device IP
192.168.13.31
AT Host Routing Mask
0.0.0.0
AT DHCP Server Mode
Enabled
DHCP network mask
255.255.255.0
AT Starting IP
192.168.13.100
Ending IP
192.168.13.150
Link Radio Coverage to Interface
Disabled
Radio Link Delay (Seconds)
10

LIITE 2

Perustietoturvan käyttöönotto Sierra Airlink Raven XE:ssä

1. Porttisuodatus otetaan käyttöön security-osion Port filtering – inbound- ja Port filtering outbound -välilehdistä. Asetetaan Port filtering mode joko **allowed-** tai **blocked**-tilaan, jolloin määriteltävät portit ovat sallittuja tai estettyjä.
2. Portit määritellään porttinumeron mukaan tietystä alueesta. Jos halutaan vain yksi portti suodatettavaksi, valitaan **start-** ja **end**-porteiksi sama arvo. Käytettäessä **allowed ports** -tilaa, on määriteltävä porteiksi myös reitittimen etähallintaan liittyvät portit. Jos käytetään IP-suodatusta ja halutaan sallia kaikki portit tietystä IP-osoitteesta, ei porttisuodatusta tarvitse välttämättä käyttää.
3. IP-osoitteiden suodatus otetaan käyttöön Trusted IPs inbound- ja Trusted IPs outbound -välilehdistä. Asetetaan sisääntulevien IP-osoitteiden suodatus päälle **Inbound trusted IPs mode** -valikoista.
4. Määritellään **Inbound trusted IPs-välilehteen** kiinteä IP-osoite, josta etähallitaan. Lisätään IP-osoite valitsemalla **add more**.
5. Tallennetaan asetukset ja käynnistetään laite uudelleen.



Etähallinan mahdollistaminen Sierra Airlink Raven XE:ssä

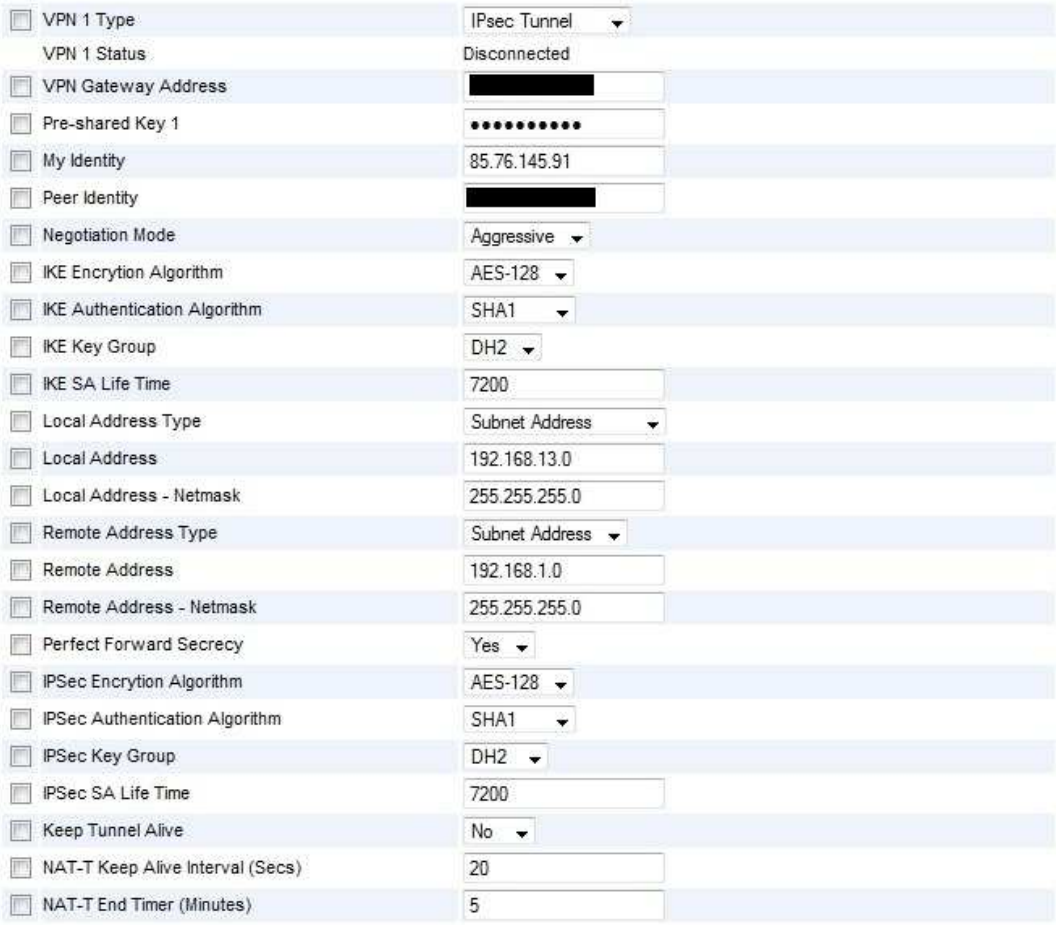
1. Mene services-välilehteen, josta valitaan **acemanager**.
2. Valitaan **enable acemanager** -valikosta **all**, jolloin reititintä voidaan etähallita ulkoverkosta.
3. Ei muuteta acemanager-porttia. Tallennetaan asetukset.
4. Vaihdetaan laitteen salasana admin-välilehdestä
5. User name ja old password ovat **user** ja **12345**, määritellään uusi salasana New password -kenttiin. Tallennetaan asetukset ja käynnistetään laite uudelleen.

LIITE 3 1/2

VPN-tunnelin käyttöönotto Sierra Airlink Raven XE:ssä

1. VPN-toiminto otetaan käyttöön VPN-välilehdestä. Global settings -välilehdestä voidaan määritellä, sallitaanko VPN-yhteyden lisäksi muita yhteyksiä Internettiin. Voidaan määritellä sisääntuleva liikenne sallituksi **Inbound out of band** -valikosta. Ulosmenevä liikenne voidaan sallia joko lähiverkon laitteille **Outgoing host out of band** -valikosta tai reitittimelle **Outgoing management out of band** -valikosta. Voidaan myös määritellä **NAT-T**-toiminto käyttöön. Varmistetaan asetukset valitsemalla **apply**.
2. Samanaikaisia VPN-tunneleita voidaan määritellä 5 kpl. Valitaan haluttu tunneli, josta voidaan tehdä joko IPSec- tai GRE-tunneli. Valitaan IPSec-tunneli.
3. Oletusasetuksina laitteessa on valmistajan oman VPN-testipalvelimen asetukset. Testataan halutessa VPN-toiminnon toiminta.
4. Asetetaan **VPN-gateway address** -kenttään käytetyn VPN-reitittimen ulkoverkon osoite.
5. **Pre-shared key 1** -kenttään asetetaan haluttu VPN-tunnelissa käytetty salasana, joka myös asetetaan VPN-reitittimeen.
6. **My identity** -kentässä tulee olla reitittimen oma IP-osoite, joka voidaan tarkistaa status-välilehdestä.
7. **Peer identity** -kenttään asetetaan myös käytetyn VPN-reitittimen ulkoverkon osoite.
8. **Negotation mode** -valikkoon asetetaan **aggressive mode**, sillä VPN-reititin tukee main mode-tilaa ainoastaan Microsoft VPN-asiakkaissa.
9. Käytetään oletusasetuksia **IKE encryption algorithm**-, **IKE authentication algorithm**-, **IKE key group**-, **IKE SA life time**-, **IPSec encryption algorithm**-, **IPSec authentication algorithm**-, **IPSec key group**-, **IPSec SA life time** -asetuksissa.
10. Määritellään local address type- ja remote address type -valikkoihin subnet address.
11. Local address-arvoksi asetetaan paikallisen lähiverkon IP-osoite **192.168.13.0**.
12. Remote address-arvoksi asetetaan VPN-reitittimen lähiverkon IP-osoite **192.168.1.0**.
13. Asetetaan **perfect forward secrecy** -valikkoon **Yes**.

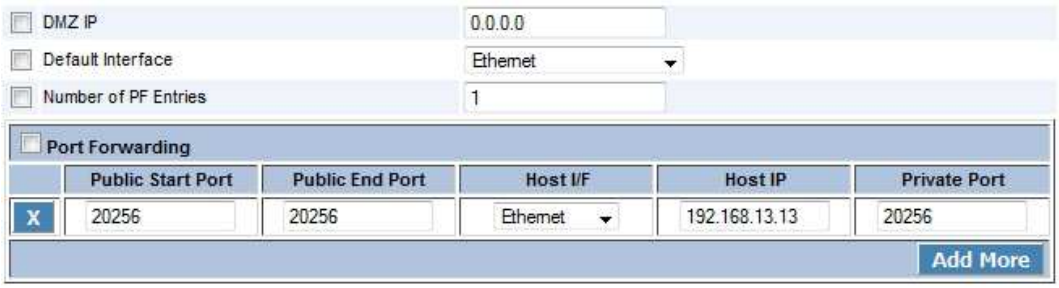
14. Aseteteaan **keep tunneli alive** -valikkoon **Yes**, jos halutaan reitittimen ottavan VPN-yhteyden automaattisesti.
15. VPN-yhteyden lokia voidaan tarkastella **log**-välilehdestä, josta voidaan myös yhdistää VPN-tunneli valitsemalla haluttu tunneli ja **connect**, jos automaattista yhdistämistä ei ole asetettu. **Log level** -valikkoon valitaan simple.



LIITE 4

Porttiohjaus Sierra Airlink Raven XE:ssä

1. Porttiohjaus otetaan käyttöön security osion **port forwarding** -välilehdestä, jos ei käytetä VPN-tunnelia.
2. Porttiohjauksessa voidaan halutessa määritellä DMZ-kohde, mutta se ei ole pakollista.
3. Oletusliitännäksi valitaan ethernet, jos käytetään ethernet-liitäntää.
4. On määriteltävä **Number of PF entries** -arvo, joka on määriteltyjen sääntöjen lukumäärä. Valitaan arvoksi **1**, sillä tehdään vain yksi sääntö valitsemalla **add more**.
5. Asetetaan ulkoverkon porttinumero **Public start port**- ja **Public end port** -kenttiin. Käytetään yhtä porttia, joten asetetaan molemmiksi arvoiksi käytettävä portti **20256**.
6. Valitaan **Host I/F**-valikossa **ethernet**.
7. **Host IP** -kentään asetetaan ohjelmoitavan logiikan IP-osoite, joka on **192.168.13.13**. **Private port** -kenttään asetetaan etähallintaohjelman käyttämä portti eli **20256**.



LIITE 5

Dynaamisen DNS:n käyttöönotto Sierra Airlink Raven XE:ssä

1. Dynaaminen DNS otetaan käyttöön services-osion dynamic DNS -välilehdestä.
2. Modem name -kohtaan määritellään haluttu verkkotunnuksen etuliite. Asetetaan **dd-c**, jolloin verkkotunnukseksi tulee **dd-c.eairlink.com**.
3. Määritellään **IP manager server 1**-kohtaan **edns2.eairlink.com**.
4. **IP manager server 1** ja **2** update-arvoiksi asetetaan **5**, joka vastaa 5 minuuttia.
5. Määritellään **IP manager server 2** -kohtaan **eairlink.com**.
6. **IP manager server 1** ja **2 Key** -arvot ovat valmiiksi määriteltyjä eikä niitä muuteta.

LIITE 6 1/2

TeleWell 3G Flash-OFDM-reitittimen käyttöönotto-ohje

1. Asetetaan USIM-kortti käytettävään 3G-modeemikorttiin, joka puolestaan asetetaan reitittimeen 3G-modeemikortin käyttämään porttiin. Halutessa USIM-kortin PIN-koodin kysely voidaan ottaa pois käytöstä matkapuhelimen asetuksista.
2. Kytketään tietokone reitittimen LAN-porttiin ja otetaan reitittimeen yhteys selaimella osoitteesta 192.168.2.254. Oletusasetuksien salasana on admin.
3. Perusasetukset voidaan määritellä joko ohjattulla käyttöönotolla tai pika-asetukset-välilehdestä. Määritellään asetukset pika-asetukset-välilehteen.
4. Valitaan ulkoverkon tyypiksi **3G** ja APN-arvoksi **internet.saunalahti**, jos liittymänä on Saunalahti. Muissa liittymissä APN:ksi valitaan **internet**.
5. Valituksi numeroksi asetetaan ***99#** ja määritellään PIN-koodi, jos se on käytössä.
6. Autentikoinniksi on valittava **CHAP**, jos käytössä on Saunalahden liittymä.
7. AT-komennoksi on määriteltävä **AT^SYSCFG=14,2,3fffffff,1,2**, jos käytetään Huawein 3G-modeemikorttia.
8. Keepalive-vaihtoehdoksi valitaan joko LCP echo request tai ping-toiminto. Ping-toiminnolle valitaan luotettava osoite kuten google.fi
9. Tallennetaan asetukset lopuksi valitsemalla tallenna. Laite käynnistyy uudelleen automaattisesti, jos muokatut asetukset sitä vaativat.
10. Jaettavat IP-osoitteet voidaan määritellä DHCP-palvelin -välilehdestä
11. WLAN-verkon asetukset määritellään ohjatun käyttöönoton yhteydessä tai langaton-välilehdestä. Valitaan SSID-tunnukseksi 3g_testi, turvallisuudeksi WPA-PSK ja salauksen tyypiksi AES. Määritellään myös haluttu salasana.

LIITE 6 2/2


►Ulkoverkon tyyppi
Kiinteä IP-osoite
Palveluntarjoaja on osoittanut sinulle kiinteän IP-osoittee
Automaattinen IP-osoite
Hae IP-osoite automaattisesti.
Automaattinen IP-osoite Road Runner istuntohallinnalla
Automaattinen IP-osoite Road Runner istuntohallinnalla
Australiassa (Telstra BigPond)
PPPoE
Jotkin palveluntarjoajat vaativat PPPoE-yhteyden käyttöä.
L2TP
Jotkin palveluntarjoajat vaativat L2TP-yhteyden käyttöä.
PPTP
Jotkin palveluntarjoajat vaativat PPTP-yhteyden käyttöä
3G
3G
FLASH-OFDM
FLASH-OFDM
►APN
internet.saunalahti
►PIN-koodi
►Valittu numero
*99#
►Käyttäjänimi
►Salasana
►Autentikointi
Automaattinen PAP CHAP
►WAN MTU
1500
►Ensisijainen DNS-palvelinosoite
0.0.0.0
►Vaihtoehtoinen DNS-palvelinosoite
0.0.0.0
►AT-komento
AT^SYSCFG=14,2,
►Automaattinen yhdistäminen
Automaattinen Manuaalinen
►Aikakatkaisun aikaraja: 300 sekuntia
►Keep Alive
Poista käytöstä
Ping-toimintoa käyttäen
►Aikaväli: 60 sekuntia
►IP-osoite:
LCP Echo Request –ominaisuutta käyttäen
►LCP-Eho aikaväli: 10 sekuntia
►LCP-Echo epäonnistuu: 3 kertaa

LIITE 7

Perustietoturvan käyttöönotto TeleWell 3G Flash-OFDM-reitittimessä

1. Saapuvien pakettien suodatus määritellään turvallisuusasetuksien pakettisuodatusvälilehdestä.
2. Valitaan saapuvien pakettien suodatus ja otetaan se käyttöön valitsemalla **päälle**.
3. Valitaan **estä muut kuin sääntöjen mukaiset paketit**.
4. Määritellään lähteen IP-osoitteeksi se, josta etähallitaan. Ei määritellä lähteen porttia, sillä sallitaan kaikki liikenne kyseisestä IP-osoitteesta.
5. Määritellään kohteen IP-osoitteeksi **192.168.2.0/24**, jolloin sallitaan liikenne kaikkiin lähiverkon laitteisiin. Ei määritellä kohteen porttia, jolloin sääntö kattaa etähallittavan laitteen lisäksi myös reitittimen käyttöliittymän etähallinnan.
6. Asetetaan sääntö käyttöön valitsemalla **päälle** säännössä. Tallennetaan asetukset.

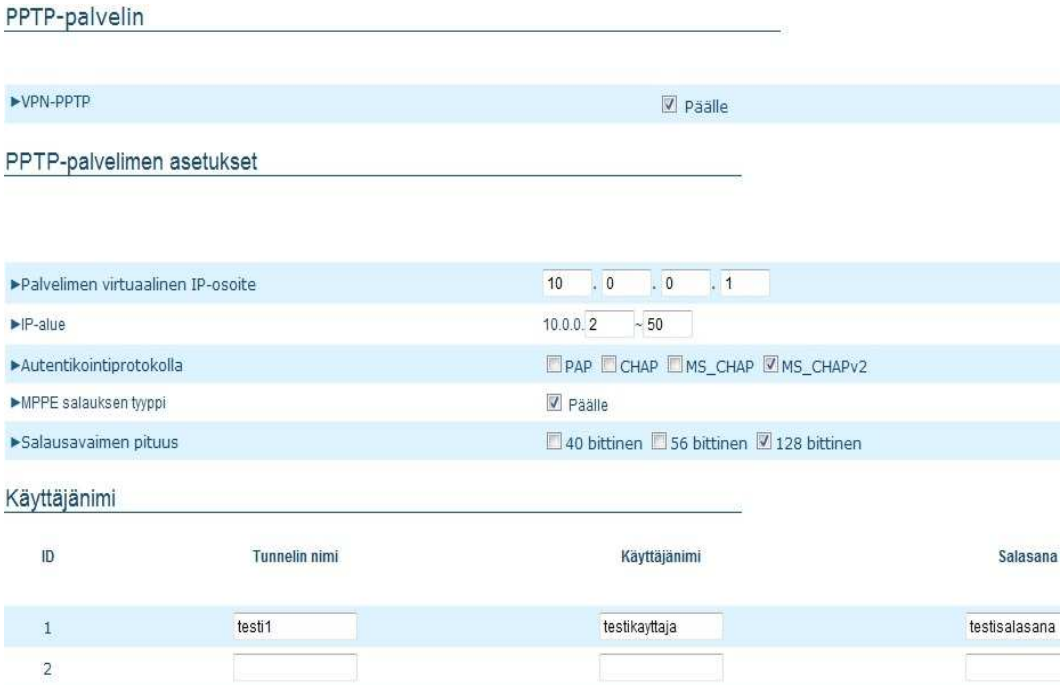
Etähallinan mahdollistaminen TeleWell 3G -reitittimessä

1. Mennään turvallisuusasetuksiin ja muut-välilehteen
2. Sallitaan etähallinta halutusta IP-osoitteesta tai isäntänimestä ja asetetaan toiminto **päälle**. Tallennetaan asetukset.
3. Voidaan asettaa toinen portti etähallintaan tai muuttaa etähallinnan aikakatkaisua.
4. Salasana vaihdetaan ensisijaisista asetuksista vaihda salasana-välilehdestä.
5. Asetetaan vanha salasana **admin** ja määritellään uusi. Tallennetaan asetukset.

LIITE 8

VPN-tunnelin käyttöönotto TeleWell 3G -reititimessä

1. Otetaan PPTP-palvelin toiminto käyttöön turvallisuusasetuksien PPTP-palvelin -välilehdestä. Asetetaan palvelin käyttöön ruksittamalla **VPN-PPTP**-valinta.
2. Ei muuteta oletusasetuksien palvelimen IP-osoitetta tai jaettavia osoitteita.
3. Valitaan käytettäväksi autentikointiprotokollaksi **MS_CHAPv2**
4. Otetaan **MPPE**-salaus käyttöön **128**-bittisellä salausavaimella.
5. Määritellään VPN-tunnelille käyttäjätili, johon asetetaan tunnelin nimi, käyttäjänimi ja salasana. VPN-asiakas kysyy ainoastaan käyttäjänimeä ja salasanaa.
6. Tallennetaan asetukset.
7. Mennään vielä muut-välilehteen, josta otetaan ruksi pois valinnasta **piilota ulkoverkon portit**. Tallennetaan lopuksi asetukset.
8. Jos halutaan käyttää reititintä PPTP-asiakkaana, valitaan PPTP-asiakas välilehti ja asetetaan asiakas käyttöön ruksittamalla **VPN-PPTP**-valinta.
9. Asiakkaalle määritellään tunnelin nimi, PPTP-palvelimen IP-osoite sekä käyttäjänimi ja salasana. Voidaan myös valita yhdistämistapa sekä asettaa MPPE-salaus ja NAT-toiminnot.



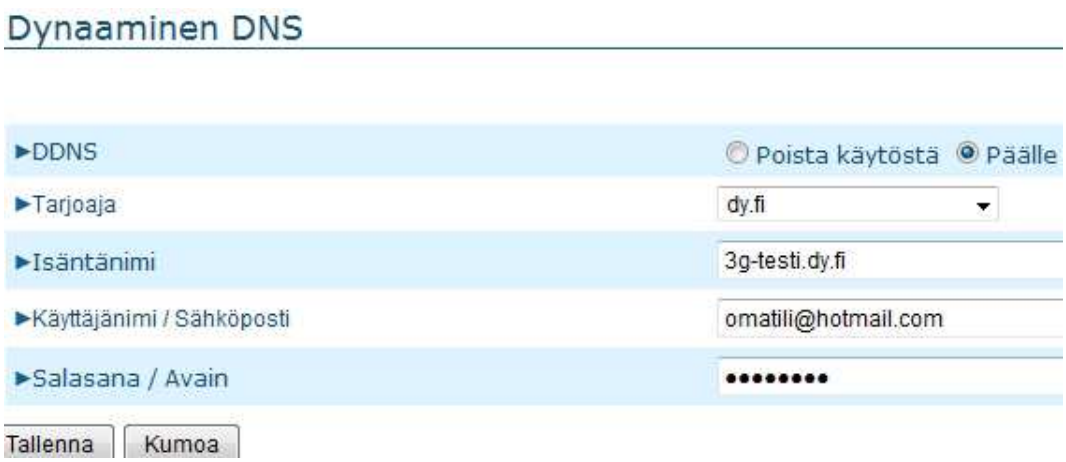
LIITE 9

Porttiohjaus TeleWell 3G -reitittimessä

1. Porttiohjaus otetaan käyttöön ohjelmallinen palvelin-välilehdestä.
2. Määritellään säännölle ulkoverkon portti **20256 palvelun portit** -kenttään.
3. Asetetaan ohjelmoitavan logiikan IP-osoite ja portti **192.168.2.13:20256** palvelimen IP- ja portti-kenttiin.
4. Otetaan sääntö käyttöön ruksittamalla **päälle**-valinta.
5. Tallennetaan asetukset.

Dynaamisen DNS:n käyttöönotto TeleWell 3G -reitittimessä

1. Dynaaminen DNS otetaan käyttöön lisäasetuksien dynaaminen DNS -välilehdestä.
2. Asetetaan **DDNS päälle** ja määritellään **palveluntarjoaja dy.fi** listasta. Käytettävä palveluntarjoaja on siis oltava jokin listan valinnoista.
3. Asetetaan rekisteröity isäntänimi **3g-testi.dy.fi**.
4. Asetetaan lopuksi rekisteröidyn tilin käyttäjänimi ja salasana.
5. Tallenetaan asetukset.



LIITE 10 1/2

IPSec-tunnelin käyttöönotto Linksys RV082 VPN-reitittimessä

1. Kirjaudutaan reitittimeen selaimella osoitteessa **192.168.1.1** käyttäjänimellä **admin** ja salasanalla **admin**.
2. Valitaan VPN-välilehti, josta puolestaan valitaan gateway to gateway -tunneli
3. Asetetaan tunnelille nimi **ipsec_testi**, **interface WAN1** ja ruksitaan **enabled**.
4. Valitaan **local security gateway type** -valikkoon **IP only** ja **local security group type** -valikkoon **subnet**. IP-osoitteeksi asetetaan **192.168.1.0**.
5. **Remote security gateway type** -valikkoon asetetaan myös **IP only** ja määritellään 3G-reitittimen osoite valitsemalla **IP by DNS resolved**. 3G-reitittimen osoitteeksi asetetaan siis **dd-c.eairlink.com**.
6. **Remote security group type** -valikkoon asetetaan **subnet** ja IP-osoitteeksi asetetaan **192.168.13.0**.
7. Keying mode -valikkoon määritellään **IKE with preshared key**.
8. Phase 1- ja phase 2 -arvoiksi määritellään samat arvot kuin Raven XE:ssä:

Phase 1 / Phase 2 DH group : Group2

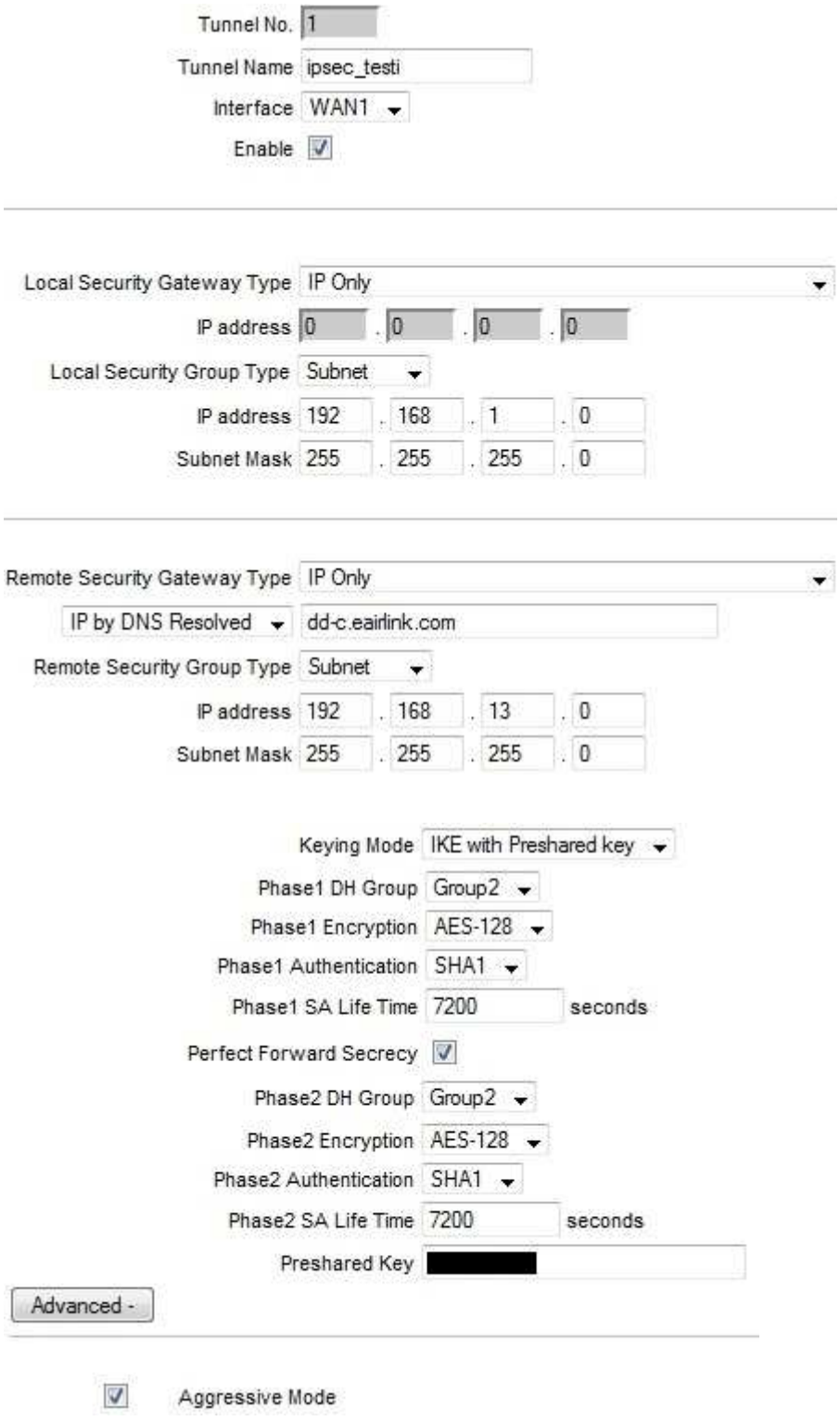
Phase 1 / Phase 2 Encryption : AES-128

Phase 1 / Phase 2 Authentication : SHA1

Phase 1 / Phase 2 SA life time : 7200

9. Ruksiteteaan **perfect forward secrecy** -valinta.
10. Asetetaan preshared key -arvoksi sama salasana kuin Raven XE:ssä.
11. Advanced-valikossa määritellään aggressive mode, koska VPN-reititin ei tue main mode-tilaa muissa kuin Microsoftin VPN-asiakkaissa.
12. Tallennetaan lopuksi asetukset valitsemalla **save settings**.

LIITE 10 2/2


Tunnel No. 1
Tunnel Name ipsec_testi
Interface WAN1
Enable
Local Security Gateway Type IP Only
IP address 0 . 0 . 0 . 0
Local Security Group Type Subnet
IP address 192 . 168 . 1 . 0
Subnet Mask 255 . 255 . 255 . 0
Remote Security Gateway Type IP Only
IP by DNS Resolved dd-c.eairlink.com
Remote Security Group Type Subnet
IP address 192 . 168 . 13 . 0
Subnet Mask 255 . 255 . 255 . 0
Keying Mode IKE with Preshared key
Phase1 DH Group Group2
Phase1 Encryption AES-128
Phase1 Authentication SHA1
Phase1 SA Life Time 7200 seconds
Perfect Forward Secrecy
Phase2 DH Group Group2
Phase2 Encryption AES-128
Phase2 Authentication SHA1
Phase2 SA Life Time 7200 seconds
Preshared Key
Advanced -
Aggressive Mode

LIITE 11

Windows 7 VPN-asiakkaan käyttöönotto

1. Mene Control panel ja valitse network and sharing center.
2. Valitse Set up a new connection or network.
3. Valitse Connect to a workplace.
4. Valitse Use my internet connection (VPN).
5. Määrittele PPTP-palvelimen osoite eli 3g-testi.dy.fi.
6. Aseta käyttäjänimi ja salasana, jotka on määritelty PPTP-palvelimelle.
7. Jos yhteys ei muodostu, mene change adapter settings.
8. Valitse properties muodostetusta VPN-yhteydestä.
9. Mene security-välilehteen ja valitse type of VPN -valikkoon PPTP
10. Valitse allow these protocols -kohtaan vain MS_CHAPv2-protokolla